Mídia Fora do Eixo | @Bicicletada 2012

ESCOLA DE ATIVISMO

[ABRINDO O CÓDIGO]

A GUIA DE FACILITAÇÃO E APRENDIZAGEM EM SEGURANÇA DA INFORMAÇÃO

A GUIA DE FACILITAÇÃO E APRENDIZAGEM EM SEGURANÇA DA INFORMAÇÃO

Este material é resultado de um compilado de estudos, informações e textos produzidos pelo Núcleo de Segurança da Informação da Escola de Ativismo, com o objetivo de subsidiar os processos de aprendizagens desenvolvidos nos últimos anos.

Mais do que a compreensão e uso correto das ferramentas de Segurança da Informação, é preciso desenvolver uma cultura de segurança que vai além do seu coletivo ou organização e se estende também à sua rede de parceiros e aliados.

A jornada de aprendizagem em segurança é um processo constante e se mostra mais eficiente quando compartilhado coletivamente. Durante este processo, tão importantes quanto os conhecimentos e técnicas de Segurança da Informação, são as habilidades de criação, facilitação e organização de processos de aprendizagem.

Este material começou a ser reunido em 2017, visando ser um ponto de partida para uma sistematização de conhecimentos relacionados à facilitação de processos de aprendizagem em Segurança da Informação. Ainda assim, alguns conteúdos são temporais e podem conter informações ou procedimentos desatualizados.

Esta Guia foi pensada para ser uma coletânea livre e em constante transformação. Corrija os textos, conteste os argumentos. Provoque-se e siga suas próprias reflexões.

Permita-se, anote, rabisque e mude a ordem, afinal, a jornada agora é sua.

Vamos juntos? Envie suas contribuições, críticas e comentários para suporte@ativismo.org.br

QUEM COLABOROU

Amarela, Carla Jancz, Carolina Munis, Fernanda Shirakawa, Foz, Gabi Juns, Gustavo Gus, Lucas Malaspina, Luciana Ferreira, Marcelo Marquesini, Narrira Lemos, Mirim, Violeta Cunha.

Revisão: Bruno Freire.

COLABORE COM ESTA GUIA

suporte@ativismo.org.br

CONTEÚDO

[introdução]

Nesta seção, preparamos uma introdução à aprendizagem de Segurança da Informação, que depende de vários fatores, do contexto sócio-político à utilização das ferramentas. Produzimos esse material para ser utilizado por grupos ativistas que tenham interesse em aprofundar, descobrir e criar metodologias próprias para a construção de processos de aprendizagem nesta área.

ÁGUIA - A GUIA

Ao passo em que o fluxo das comunicações da sociedade se dá cada vez mais no ambiente digital, a vigilância e o monitoramento se tornaram práticas valiosas e bastante comuns no campo das disputas políticas e sociais.

Por que Águia - A Guia?

Segundo dicionário de símbolos, a águia é um animal solar e celeste, símbolo da força, vitalidade e proteção. Muito ágil e habilidosa, essa ave também está relacionada à realeza e aos Deuses pela perspicácia de seu olhar, pois ele lhe permite fitar o Sol diretamente. Um símbolo de clarividência.

É considerada um animal psicopompo, do grego *psychopompós*, união das palavras *psykhé*, que significa "alma", e *pompós*, que significa "guia". A águia, assim, carrega o sentido de orientar situações de iniciação ou de transição.

Neste sentido, a nossa Guia pretende ser uma ÁGuia. Por servir de orientação, uma referência para que seus estudos e aprendizados sobre o campo da Segurança da Informação não fiquem restritos, mas que você possa carregá-la e recorrer a ela quando necessário.

Neste material, você encontrará algumas possibilidades de leituras como uma base de sustentação para os movimentos do pensamento e da ação com organizações e coletivos. Contém, ainda, referências para que você construa a sua oficina ou atividade considerando aspectos básicos ou mais sofisticados, dependendo do grupo e da necessidade.

Tudo isso de um modo inventivo: este é o jeito que a Escola de Ativismo encontra para realizar seus processos de aprendizagem, incentivando a multiplicação, a edição e a produção de conhecimentos.

A Guia pretende ser também uma referência em um modo de realizar processos formativos que incentiva a inquietação, com práticas de ampliação da experiência das pessoas participantes com o pensamento e com a ação. Ela nos convida a formular boas perguntas ao invés de ser somente um caderno com receitas. Ela indica pistas para um caminho que se faz na própria caminhada mais do que trajetórias definidas.

Desejamos a você uma ótima experiência de leitura, estudos e aprendizados!

Escola de Ativismo
16 de Setembro de 2017

APRENDIZAGEM EM SEGURANÇA DA INFORMAÇÃO

O contexto da aprendizagem em Segurança da Informação.

Em um universo tecnológico cada vez mais dilatado, a aprendizagem em Segurança de Informação (SI) acontece na forma de um desafio. Nossa compreensão é de que ela ocorre somente se houver uma necessidade, um desejo em aprender, seja para proteger a si mesmo, algo ou alguém, seja para atualizar-se, seja para romper com certas estruturas de captura do pensamento e dos corpos.

Um segundo fator importante neste processo é a compreensão de que vivemos em constante processo de alfabetização, como diria o educador Álvaro Vieira Pinto, pois nunca seremos alfabetizados em todos os temas ou assuntos. Haverá sempre algo novo a aprender e também a ensinar.

E um terceiro fator considerável para a aprendizagem em SI são os métodos utilizados. Sabemos que, em nosso cotidiano, são oferecidos meios diversos para facilitar a vida. Nossa experimentação fica reduzida a algo que seja prático, rápido e de fácil absorção, portanto, estamos cada vez mais distantes de um processo de aprendizado complexo. Nesse sentido, é preciso realizar uma compreensão política destes sistemas e ferramentas, para iniciar um processo de distanciamento do que nos é oferecido e uma transição para outros sistemas. Trata-se de evitar instrumentos de captura e vigilância por meio do conhecimento de ferramentas que visam independência das estruturas de poder, o que exige dedicação e atenção por parte do aprendente.

Assim, é necessário que as ferramentas de Segurança de Informação sejam apresentadas junto com o contexto vivenciado, impulsionando uma problematização de sua utilização. O acompanhamento desse processo também é fundamental, é preciso ter alguém que entenda do assunto a quem se recorrer quando surgirem dúvidas ou algo emperrar no caminho.

A aprendizagem em Segurança da Informação poderá se tornar significativa se houver mútua implicação entre: as necessidades da pessoa aprendente, a compreensão do contexto social, político, tecnológico e ambiental e o oferecimento de ferramentas funcionais com o devido acompanhamento em sua implementação.

Mídia Ninja | #PasseLivre 2017

[pré-oficina]

Antes de realizar uma oficina, recomendamos pensar e elaborar alguns pontos para a sua realização. Estes pontos podem ser reflexões para as seguintes perguntas: quando precisamos de uma oficina em Segurança da Informação? Por onde começar? O que precisamos para torná-la possível? Além disso, trazemos também uma sugestão de construção de roteiro, que poderá ajudar você a construir a metodologia e visualizar o andamento das atividades.

QUANDO FAZER UMA OFICINA

A aprendizagem em Segurança da Informação pode acontecer de diferentes maneiras. Uma possibilidade é utilizar o modelo de oficina, que permite um compartilhamento de experiências e realidades entre as pessoas participantes e que, se bem conduzida, pode criar um ambiente em que todos aprendem com todos e fazer emergir boas possibilidades de uso da SI pelo grupo. Mas quando e como fazer uma oficina?

A aprendizagem em Segurança da Informação para adultos envolve mudança de hábitos, de crenças consolidadas e até mesmo de cultura em relação à tecnologia. Envolve compreender o que é ou não risco e ameaça para você, seu grupo e suas atividades.

O modelo de oficina prevê uma interação maior entre a(s) pessoa(s) facilitadora(s) e as pessoas participantes do processo de aprendizagem, e deve ser pensado sob essa perspectiva. Mas a aprendizagem começa com o interesse da pessoa ou grupo aprendiz. E esse interesse pode advir de vários fatores: necessidade, curiosidade ou desejo de saber mais sobre o tema em questão.

O grau de interesse do grupo a ser beneficiado afetará diretamente a decisão de optar ou não por fazer uma oficina num dado momento. Portanto, antes de tomar a decisão de fazer uma oficina, cheque o grau de interesse de seu grupo ou das pessoas que participarão do processo em relação ao tema a ser abordado.

Verifique, ainda, quais as necessidades específicas de aprendizagem que elas têm. Isso pode ser feito por meio de questionários, entrevistas, acompanhamento das pessoas em seu dia a dia, pesquisa direta ou - menos eficiente - informações secundárias prestadas por alguém ou adquiridas em relatórios e outras fontes. Esses mecanismos já podem ser um primeiro canal de envolvimento das pessoas.

O interesse e a necessidade influenciam o desenho da sua oficina e a escolha das pessoas facilitadoras. Eles pode determinar, por exemplo, se você precisará trabalhar mais com informações gerais e de contexto para gerar sensibilização e envolvimento com o tema em questão. Ou, em outro extremo, se já é o momento de priorizar as atividades focadas nas soluções e das mudanças desejadas, como instalação e uso de novos aplicativos (*apps*) e programas (*softwares*) e mudanças de rotinas e hábitos.

Lembre-se que o tema abordado e o método utilizado precisam ser bem pensados e definidos. Uma oficina não deve ser uma sequência de palestras encadeadas a partir de uma certa lógica. Ela pode ter interação, espaços de compartilhamento e ser inclusiva! Cada pessoa adulta tem sua maneira única de aprender. As pessoas com mais dificuldade na aprendizagem podem se tornar as mais vulneráveis.

Facilite a participação através de debates, jogos, atividades lúdicas e outras ferramentas. Quanto mais as pessoas se sentirem envolvidas e ativas no processo, maior será a chance da oficina atingir seus objetivos.

Caso você detecte que o interesse dos potenciais participantes não é suficiente para a realização de uma oficina, outras alternativas iniciais podem ser exploradas: promover rodas de diálogos sobre o tema, distribuir textos, disponibilizar vídeos, convidar pessoas para darem palestras, etc. Em suma, criar um clima!

Por fim, tenha em mente que a aprendizagem em Segurança da Informação depende, acima de tudo, de mudanças de comportamento, cultura e hábitos a nível individual e, principalmente, de grupo. Uma oficina, por si só, não é suficiente para engendrar essas transformações. Por isso, considere a aprendizagem como um processo de médio a longo prazo. Comece aos poucos, planeje um objetivo simples para sua oficina e insira-a dentro de uma estratégia mais ampla de aprendizagem.

PLANEJANDO UMA OFICINA

Como planejar um processo de aprendizagem: as 3 fases e os momentos essenciais de uma oficina.

Uma forma eficaz de estruturar o planejamento de uma oficina de Segurança da Informação é dividir o processo em 3 etapas: PRÉ-OFICINA, DURANTE A OFICINA e PÓS-OFICINA.

Cada processo de aprendizagem terá suas necessidades e características próprias, mas algumas atividades são comuns a vários tipos de oficina. Vamos resumir cada uma destas etapas, incluindo algumas perguntas que lhe ajudarão a pensar e organizar este processo.

PRÉ-OFICINA:
A etapa "pré-oficina" vai desde o momento em que a oficina é concebida como proposta até a recepção das pessoas participantes. Normalmente, envolve fazer uma boa avaliação das necessidades do coletivo, planejar o roteiro, levantar as necessidades de espaço e de materiais e se comunicar com os participantes de maneira minimamente segura.

Quais são as principais necessidades do grupo? Verifique as demandas que o grupo encontra em seu cotidiano e seu trabalho e transforme-as em necessidades de aprendizagem.

Quais hábitos e práticas as pessoas participantes possuem atualmente? Pesquise o perfil, a infraestrutura digital utilizada e os hábitos digitais das pessoas participantes. É fundamental saber os sistemas operacionais utilizados, para certificar-se de que as pessoas facilitadoras dominam seu funcionamento e o das ferramentas que se adaptam a eles.

Qual o grupo de pessoas facilitadoras necessárias para realizar a oficina? Pense nos perfis necessários e no número de pessoas suficiente para um acompanhamento adequado do grupo.

Quais habilidades e conhecimentos queremos desenvolver até o final do processo? Estabeleça objetivos de aprendizagem baseados nas necessidades do grupo e no que você e sua equipe podem oferecer. Mas lembre-se: no momento da oficina, aparecerão fatores inesperados ou não detectados antes. Por isso, mantenha uma abertura para redimensionar esses objetivos durante a oficina e transforme as surpresas em riquezas. O processo é vivo!

Quais reflexões e encadeamento de ideias queremos provocar em cada sessão? Desenhe um roteiro que conduza aos objetivos de aprendizagem de forma fluida e satisfatória. E, novamente, é importante estar de prontidão para mudar o percurso caso a necessidade do grupo mude durante a oficina. Veja mais na seção "Roteiro".

Que materiais serão necessários para desenvolver cada atividade? Uma dica é elaborar um roteiro de oficina que contenha as dinâmicas propostas e os materiais que cada uma delas utilizará.

Quantos recursos financeiros serão necessários para a realização da oficina? Considere remuneração ou ajuda de custo para as pessoas facilitadoras, alimentação, transporte e outros itens.

Quais procedimentos logísticos serão necessários para conduzir a oficina? Veja mais na seção “Preparando uma oficina: A logística operacional”.

DURANTE A OFICINA:
A etapa “durante a oficina” vai desde a recepção dos participantes até a sessão de fechamento e contém tanto as atividades de aprendizagem quanto os momentos entre as sessões. Toda a interação entre o grupo e entre as pessoas facilitadoras é uma oportunidade de aprendizagem. Por isso também é importante realizar conversas entre o grupo de facilitação que está conduzindo o processo a fim de avaliar o andamento das atividades e aprimorá-las para que as necessidades do grupo sejam atendidas.

Como está a energia e o nível de atenção do grupo? As pausas são tão importantes quanto as sessões. É nelas que a equipe facilitadora detecta como o grupo está, quem está conseguindo acompanhar e quem está com dificuldade. Procure detectar a necessidade de dar um intervalo ou de mudar a energia da sala.

Como manter o clima e a atenção nas atividades? Saber identificar que tipo de “clima” cada sessão exige e mantê-lo é uma parte fundamental da aprendizagem. Algumas sessões pedem um ambiente mais silencioso, meditativo e propício para a concentração profunda. Outras pedem mais dinamismo, participação e movimento. Pense em maneiras criativas de atender a isso!

Como seguir ativando e envolvendo o grupo? Em sua oficina, evite tentar envolver ou sensibilizar as pessoas participantes por meio do “susto”, ou seja, usando o medo do monitoramento, da vigilância ou ainda da citação de casos reais de quebra de segurança. O risco é alto de muitas pessoas optarem pela alienação, descrédito ou contestação pura e simples e não se abrirem para a aprendizagem.

Como vamos monitorar se as pessoas participantes estão aprendendo? Construa formas de avaliação e acompanhamento da aprendizagem enquanto a oficina acontece.

Como está a equipe de facilitação? A equipe precisa verificar constantemente como estão as pessoas integrantes: se há sentimentos de sobrecarga, ansiedade, frustração, ou mesmo confiança excessiva. Esse auto-cuidado e cuidado de si é essencial para um bom ambiente de aprendizagem e para que as pessoas facilitadoras consigam se conectar com as necessidades do grupo.

Os objetivos de aprendizagem desenhados inicialmente ainda fazem sentido? Reúna a equipe em momentos-chave durante a oficina para avaliar se os objetivos, desenhados a partir das necessidades identificadas na etapa pré-oficina, ainda correspondem à realidade trazida pelo grupo durante a oficina.

O roteiro original ainda faz sentido? Verifique se as sessões propostas de fato conduzirão aos objetivos, principalmente se eles foram redesenhados.

PÓS OFICINA:
O desenvolvimento dos conhecimentos e habilidades não se encerra ao final de uma oficina. É importante estabelecer algum tipo de suporte e acompanhamento da evolução do grupo. A criação de canais de comunicação

ou a produção de materiais de apoio e outras formas de suporte à aprendizagem são essenciais para ajudar na jornada de aquisição de conhecimento.

O grupo necessitará de acompanhamento pós oficina? A necessidade de acompanhamento pode vir de vários fatores, como o uso de ferramentas recém-instaladas, apoio na multiplicação dos conhecimentos para os coletivos e organizações das pessoas participantes ou ajuda para pessoas que não tiverem consolidado o conhecimento em um ou mais tópicos da oficina.

Quais recursos e sistemas precisamos criar para executar esse acompanhamento? Planeje os canais de comunicação, plataformas, materiais, tempo e recursos financeiros necessários para realizar o acompanhamento.

PREPARANDO UMA OFICINA: A LOGÍSTICA OPERACIONAL

Para preparar uma oficina é preciso, antes de mais nada, entender qual é a demanda do grupo, do local e do tempo necessário. As listas de checagem, ou checklists, são as grandes aliadas para garantir que nada seja esquecido. A comunicação com as pessoas envolvidas também é uma prática fundamental, seja com o grupo de participantes ou de facilitadores. E, na dúvida, sempre pergunte!

É fundamental que a pessoa ou equipe responsável pela logística esteja em contato constante com as pessoas facilitadoras da oficina. Assim, ela poderá entender qual o objetivo do encontro, qual a sua duração prevista, quais as demandas de estrutura necessária, o tamanho do grupo e o perfil das pessoas participantes.

O melhor recurso para o acompanhamento das necessidades logísticas é a lista de checagem, ou *checklist*, que ajuda a garantir que nada seja esquecido.

Qual o objetivo da oficina? O objetivo pode influenciar o local escolhido, a forma como é feita a comunicação com as pessoas participantes e os recursos necessários.

Qual o orçamento disponível para a oficina? Verifique o orçamento total e o orçamento para cada item, como alimentação, transporte, local e seguro (se houver). Acompanhe a execução de cada gasto e, se necessário, negocie com a equipe facilitadora a transferência de recurso de um item para outro.

Qual o tamanho e o perfil do grupo? Pergunte sobre idade, necessidades especiais, dieta vegana ou vegetariana, restrições alimentares, alergias, doenças crônicas, contato de emergência e outros fatores. Outro ponto a se notar é que as necessidades de comunicação e relacionamento com o grupo mudam se as pessoas participantes forem da mesma organização que você, de outra organização única ou de diferentes organizações e localidades.

Como será a alimentação durante a oficina? Caso a oficina for fornecer alimentação, certifique-se de que há louça e cozinha de apoio no local escolhido. E, principalmente, prepare um cardápio que se encaixe no orçamento e nas necessidades das pessoas participantes. Por fim, não se esqueça de planejar o fornecimento de água potável e do bom e velho café!

Qual o local ideal para a oficina? O local deve atender todas os fatores listados acima. E, ainda, tenha certeza de que ele atende demandas básicas, como: mesas, cadeiras, tomadas, quadro negro/branco, flip chart, projetor, caixa de som, parede para projeção, parede para colar tarjetas e/ou cartazes e espaço para trabalhos em grupo e em plenária.

É importante conferir também o estado dos banheiros, ventilação, iluminação e interferências externas, como barulho da rua. Além disso, procure garantir que no dia do encontro tudo esteja limpo e em ordem.

Faça pelo menos uma visita técnica ao local, de preferência no mesmo dia da semana e horário em que a oficina ocorrerá para saber o que esperar.

O grupo precisará de seguro de vida ou equipamentos? Prevenir incidentes pode trazer mais tranquilidade e menos custos. Caso o seguro seja uma possibilidade, verifique se há orçamento disponível para tanto e reúna as informações necessárias (veja mais sobre como armazenar essas informações na seção “Comunicando-se de maneira segura com as pessoas participantes”).

Quais materiais serão necessários? Peça à equipe facilitadora que liste todos os itens necessários e providencie-os. Por exemplo: internet, papel sulfite, canetas, pincéis atômicos, giz para quadro, fita crepe, crachás, extensões, materiais impressos, etc.

COMUNICANDO-SE DE MANEIRA SEGURA COM AS PESSOAS PARTICIPANTES

É comum que pessoas que participam de processos de aprendizagem em Segurança da Informação se preocupem com a segurança das suas comunicações ou estejam em situação de ameaça ou monitoramento. Assim, é importante oferecer a escolha de ferramentas seguras para a comunicação que precede a oficina, certificando-se que as pessoas participantes querem e sabem utilizá-las.

Planeje e prepare-se para fazer contato constante com as pessoas participantes da oficina. É comum que elas tenham diversas perguntas, pedidos e comentários no período anterior ao processo. Se possível, tenha alguém com dedicação exclusiva para isso.

Tente entender o contexto em que as pessoas participantes estão inseridas, o grau de segurança necessário para cada uma delas e o quão confortáveis elas estão em usar ferramentas de comunicação mais seguras. Caso as condições e necessidades levem à opção por ferramentas mais seguras, explique isso forma clara e resumida. Evite canais de comunicação como *Whatsapp*, *Facebook* ou *Gmail* e direcione as pessoas para ferramentas como *Jitsi* (para conversas de áudio e vídeo online), *Signal* (para chat no celular ou desktop) ou email criptografado de e-mail (auxilie na criação de uma conta de e-mail no *Riseup*). No entanto, certifique-se sempre de que o uso destes recursos é viável para a pessoa participante e não irá impedir sua comunicação com ela, especialmente na importante etapa pré-oficina.

Ao passar a reunir dados e informações de diferentes pessoas, principalmente de ativistas, é muito importante que você tenha um protocolo de segurança. Tanto a sua lista de possíveis participantes ou de convidados como a lista de participantes confirmados na oficina devem estar salvas de maneira segura. A menos que esteja usando um servidor de confiança para armazenamento online, opte por pasta criptografada no seu computador e acesse preferencialmente offline. Evite relacionar o nome das pessoas à área de atuação ou região em que vive, e aproveite para soltar a imaginação e criar apelidos para identificar os participantes em suas listas.

O local e data de realização da oficina também são informações muito sensíveis e requerem cuidado. Tente divulgar isso aos participantes o mais próximo possível da data da realização: assim, evita-se que o local vire alvo de atenção ou tentativas de interferência. Uma dica é avisar com antecedência a região em que a oficina acontecerá, sem endereço exato, e comunicar a localização exata apenas quando os participantes estiverem prestes a sair de casa, em caso de transporte individual, ou já a caminho do encontro, em caso de transporte coletivo. Quando fizer isso, organize as informações mais importantes em um informativo que deve ter no mínimo: *data e horário, local, como chegar, o que a pessoa participante precisa levar.*

ROTEIRO

Elaborar um roteiro vai te ajudar a planejar o tempo da atividade ou oficina e a lembrar do que você precisa fazer. É como um roteiro regular, mas inclui tempo, objetivo, materiais que você vai precisar e o conteúdo que você irá cobrir.

Como uma pessoa facilitadora em Segurança da Informação, você será muitas vezes quem vai introduzir, pela primeira vez, alguém no mundo da segurança digital; o que você diz terá um grande impacto em como as pessoas pensam a respeito desse tema. Um péssimo primeiro treinamento de segurança pode ser tão ruim quanto ou pior que nenhum treinamento! Sem uma estrutura, facilmente podemos nos perder dos objetivos da atividade e prejudicar nosso público, mais do que conquistá-lo. Por isso, é necessário um treinamento bem estruturado, com o tempo, os objetivos e os resultados que se deseja alcançar..

É importante que a estrutura do seu treinamento leve em consideração o objetivo de cada atividade e, consequentemente, varie em relação a ele. Além disso, o tempo disponível para realizar a atividade, o espaço para realizá-la e os materiais disponíveis também interferem no processo em si. A depender do tamanho e do tempo da oficina (de algumas horas, de um dia, de três ou até de dez dias), você pode construir um roteiro resumido e/ou um roteiro detalhado. O roteiro resumido pode ser entregue para as pessoas participantes da oficina, enquanto o detalhado poderá ser usado por você ao longo da atividade.

Geralmente, dividimos nosso roteiro de atividades ou oficina com base em sessões, então, se você planejou um dia de várias oficinas/sessões, poderia construir um roteiro para cada uma delas. Temos um exemplo que pode ser usado como base para você construir um roteiro para seu grupo - mas lembre-se de adaptá-lo da maneira que for melhor para você e seu grupo.

SUGESTÃO DE ROTEIRO

SESSÃO: Coloque aqui o nome da sua sessão. Ex: Introdução à SI ou Criptografia de E-mails.

Nº. DE PARTICIPANTES: É importante saber quantas pessoas vão participar da sua oficina, para saber, também, quantas pessoas serão necessárias na facilitação. Se for uma oficina de instalação por exemplo, sugerimos 1 pessoa facilitadora para cada 5 participantes.

OBJETIVO: Descrever o objetivo desta sessão. Isso ajudará você a pensar como organizá-la e, também, avaliar, ao final, se conseguiu alcançar a sua proposta. Iniciamos os objetivos sempre com verbos: Alcançar, proporcionar, vivenciar, mostrar, criar, registrar, e outros que mostrem a intencionalidade de uma ação.

CONTEÚDOS: Os conteúdos referem-se aos temas trabalhados. O conteúdo da oficina é de introdução, básico, intermediário, avançado? Qual é o tema principal? Quais são os temas secundários?

METODOLOGIA/COMO FAZER: *Metodologia* é uma palavra derivada de "método", do Latim "methodus" cujo *significado* é "caminho ou a via para a realização de algo". Esta parte é muito importante. É onde descrevemos, passo a passo, como a atividade será realizada, incluindo o tempo que será gasto em cada ponto. Fique atento nesta descrição para que ela ajude no momento da realização da atividade. A mensuração do tempo é importante, mas não pode ser uma prisão. Sempre é possível rever ou alterar o tempo de acordo com o andamento da aprendizagem e do grupo. Fazer o roteiro tem o objetivo de ajudar você durante a oficina, e não o contrário.

Exemplo de descrição do método e tempo:

Sessão 1:

> Explicar como vai funcionar a atividade. Dividir as pessoas participantes em grupos. 5'
> Iniciar a conversa baseada na primeira rodada de perguntas. 20'
> Inserir a segunda rodada de perguntas como estímulo para continuidade da conversa. 10'
> Inserir a terceira rodada de perguntas como estímulo final para conversa. 10'
> Pedir para cada grupo sintetizar sua compreensão sobre o tema. 5'
> Para finalizar, cada grupo compartilha sua síntese. 3' por grupo
> Espaço final livre para comentários com falas individuais. 2' por pessoa.

REFERÊNCIAS: As referências podem ajudar você a construir o conteúdo e, além disso, a auxiliar a próxima pessoa que vai fazer essa sessão.

TEMPO: Coloque aqui o tempo total da sessão.

MATERIAIS: Liste os materiais que serão usados (quantidade de mesas, cadeiras, cartolinas, canetas, post-it, entre outros).

DICAS: Fazer uma boa seleção de perguntas como estímulo e provocação para conversas. Ter perguntas adicionais/alternativas para dinamizar as conversas de acordo com o perfil das pessoas participantes. Adaptar o tempo de duração da sessão de acordo com o número de participantes. Imprimir a quantidade de perguntas de acordo com o número de grupos.

TAGS: Quais são as principais categorias desta sessão? Liste aqui (exemplo: segurança, criptografia, e-mail, etc).

AGORA NA PRÁTICA
EXEMPLO DE ROTEIRO PARA PREENCHER

SESSÃO:

Nº. DE PARTICIPANTES:

OBJETIVO:

CONTEÚDOS:

METODOLOGIA/COMO FAZER:

REFERÊNCIAS:

TEMPO:

MATERIAIS:

DICAS:

TAGS:

[durante a oficina]

Uma oficina em Segurança da Informação é um encontro de pessoas tentando aprender mais e juntas. Durante a oficina, facilitadores e participantes procuram interagir em simbiose. Nesta seção, damos algumas dicas para que isso aconteça em harmonia em ambos os grupos, como o alinhamento de expectativas e a construção de acordos.

Israel Campos | @Bloco Sagrada Profana 2017

MOMENTO INICIAL

O Momento Inicial é essencial para ganhar a confiança do grupo e estabelecer um ambiente com bons vínculos para aprendizagem.

A Abertura, ou Momento Inicial da Oficina, é fundamental para estabelecer as expectativas e criar um ambiente acolhedor de aprendizagem entre as pessoas participantes. Criar as bases de confiança entre elas e a equipe de facilitação é essencial para o bom andamento da oficina. Durante o Momento de Abertura, devem ser considerados os seguintes passos:

- Apresentações da equipe que organiza e facilita a atividade ou oficina;
- Apresentação das pessoas participantes
- Expectativa das pessoas participantes
- Programa ou roteiro do encontro
- Informações logísticas e outras informações relevantes

Fala Inicial da equipe sobre a atividade
A fala inicial da equipe é importante para dar as boas vindas às pessoas presentes e ajudar a estabelecer em bom ambiente para o início das atividades.

Apresentação da equipe ou pessoa facilitadora
A apresentação da equipe ou pessoa facilitadora serve para compartilhar com o grupo os papéis e funções de cada pessoa durante a oficina. A pessoa facilitadora pode incluir um breve resumo de sua experiência no tema, se achar necessário.

Apresentação das pessoas participantes
No campo da Segurança da Informação, as pessoas participantes podem ser mais resistentes ao compartilhamento de informações pessoais nos primeiros instantes da oficina. Uma ideia é começar com atividades de reconhecimento de grupo, como agrupar pessoas por hábitos similares. Outra dica é iniciar as apresentações em grupos menores antes de as pessoas participantes se apresentarem para o grupo todo. No caso de grupos de conhecidos, esta sessão pode ser adaptada, como por exemplo a partilha de um assunto em duplas que depois é compartilhado.

Alinhamento de expectativas
Toda pessoa participante chega ao evento com uma série de expectativas e necessidades, que podem ou não coincidir com os objetivos gerais da oficina. É importante que as expectativas sejam declaradas e, dentro do possível, incorporadas à oficina. Os acordos comuns, quando ficam visíveis para todo o grupo, geram responsabilidade compartilhada sobre os objetivos da atividade.

Leitura coletiva do programa ou roteiro do encontro
Fazer uma leitura coletiva da agenda do dia, destacando os tópicos principais, os objetivos de cada sessão e os resultados esperados ajuda a minimizar a desconfiança e insegurança das pessoas participantes nos primeiros momentos da oficina.

Informações logísticas e acordos de convivência e segurança

Reserve um momento para esclarecer e entrar em acordo sobre as principais questões logísticas e operacionais da oficina:

> Apresentação geral do local
> Acomodações, caso haja pernoite
> Horários de início, encerramento e intervalos
> Alimentação
> Transporte de volta
> Pactos de segurança (veja mais na seção “Comunicando-se de maneira segura com as pessoas participantes”)

ACORDOS DE CONVIVÊNCIA E ESPAÇO SEGURO

Garantir um espaço seguro para a troca de experiências e o compartilhamento de conhecimentos é importante para o bem estar do grupo e fundamental para a aprendizagem.

No contexto da aprendizagem adulta e principalmente no tema de Segurança da Informação, a relação estabelecida entre a equipe de facilitadores e as pessoas participantes deve ser mais uma parceria do que uma relação hierárquica. A construção de confiança e respeito mútuo entre o grupo são essenciais para o bom desenvolvimento da oficina, uma vez que oficinas de SI normalmente tratam de informações sensíveis e que podem colocar não só as pessoas participantes, mas todos os indivíduos envolvidos em risco.

Visando garantir um espaço seguro para a troca de informações e aprendizagem, o grupo pode construir acordo sobre regras mínimas de convivência. Tais acordos são levantados pelas próprias pessoas participantes e discutidos com o grupo até que se alcance consenso ou consentimento. Os acordos devem permanecer visíveis para as pessoas participantes durante toda a oficina e qualquer pessoa pode chamar a atenção do grupo para uma das regras caso sinta que ela tenha sido violada. Os tópicos a seguir podem servir como ponto de partida para a construção desse acordo, mas é importante que sejam explorados também outros tópicos relacionados ao contexto específico da sua oficina.

Cumprimento de horários e pontualidade: Acordos sobre o horário de início, encerramento e duração das sessões, incluindo intervalos, refeições etc.

Presença e participação: As pessoas participantes devem se comprometer a estar presentes física e mentalmente em todas as sessões, com atenções especiais para navegação na internet, checagem de e-mails e utilização de redes sociais.

Computadores e telefones: Quando necessário, deve existir um acordo sobre a utilização de computadores e telefones durante as sessões, bem como o que fazer quando o uso desses aparelhos não for permitido.

Fotos e redes sociais: Oficinas de Segurança da Informação normalmente são eventos sigilosos, porém esse costume nem sempre é conhecido entre todos os participantes, por isso é importante pactuar sobre questões como a realização de fotos e/ou postagens nas redes sociais sobre o evento. Caso postagens sejam permitidas, é importante decidir também sobre marcações e localização. E, caso fotos sejam permitidas, vale especificar de quem, quando e onde.

Segurança Física: A segurança física das pessoas envolvidas em uma oficina deve ser uma responsabilidade compartilhada entre o grupo todo. Portanto, é importante estabelecer um pacto de não praticar nenhum ato que ponha a segurança de alguma outra pessoa participante, organizadora ou facilitadora em risco, bem como o acordo máximo de não colocar fogo na oficina.

Política anti-downloads: Construir um pacto de bom uso da internet disponível é essencial para o sucesso de uma Oficina de Segurança da Informação. Isso significa garantir que programas que possam afetar a conexão dos demais participantes estejam desligados, como Torrents, sincronizações de Dropbox, Google Drive e quaisquer outros serviços que possam gerar tráfego em

segundo plano, bem como alertas e notificações que possam interromper o bom andamento das atividades.

Responsabilidade sobre a própria aprendizagem: Responsabilidade com a própria aprendizagem é um acordos indispensável. Uma boa conversa sobre as necessidades individuais e acordos coletivos é sempre boa pedida em imersões, oficinas e atividades.

Respeito a questões de raça, etnia, gênero, identidade de gênero, orientação sexual, regionalidade e capacidade: A diversidade é, antes de tudo, uma riqueza e um ativo de qualquer ambiente de aprendizagem. Para tratá-la como tal, é importante começar conversando coletivamente sobre o respeito e valorização da singularidade de cada pessoa e termos e posturas que não devem ser empregados.

ENCERRAMENTO - MOMENTO FINAL
AVALIAÇÃO DE APRENDIZAGENS

A palavra avaliação deriva do latim: VALERE, "ser forte, estar bem, ser de valor". Ou seja, avaliação nos remete a atribuir valor a alguma coisa ou a alguém. Mesmo sem um ambiente definido, estamos em constante avaliação, avaliamos nosso dia, nossas atividades, o que vamos comer, o que vamos vestir. A avaliação pode ser compreendida como parte da aprendizagem. Os espaços de avaliação são, portanto, espaços para apontar elementos que agregaram valor a uma pessoa ou grupo, sendo bastante utilizados para replanejar ações, atividades e procedimentos.

Avaliação dos participantes:
O momento de avaliação de uma atividade ou oficina é uma etapa do processo de aprendizagem tanto para participantes quanto para a equipe que oferece a atividade.

Ela oferece possibilidades para problematizar o espaço, os métodos, o conteúdo, a facilitação ou mediação de um processo, os materiais disponibilizados, a alimentação e tantos outros elementos que se deseja saber, medir ou atribuir valor com o grupo.

Na residência de SI, o processo de avaliação ocorre a partir de uma metodologia denominada *Contorno*. Nela, as pessoas participantes realizam o contorno de seus corpos e à medida que as atividades vão acontecendo, realizam representações no contorno com o apoio de recortes, desenhos e símbolos desenhados na folha. Os *Contornos* ficam expostos durante toda a residência, e é por meio dele que participantes e equipe acompanham os processos de aprendizagem de cada pessoa e do grupo como um todo.

Este tipo de atividade confere um modo diferente de realizar processos de avaliação, que mensura a aprendizagem para além da linguagem falada tradicional. Ele procura escapar dos modos convencionais de transmitir informações sobre determinada situação e não impede que a partilha sobre os afetos e sobre os aprendizados aconteça. Pelo contrário, é válida a utilização da imagem para realizar uma boa conversa.

Em oficinas ou atividades de curta duração, realizar o *Contorno* pode ser difícil por conta do tempo. Então, pode-se realizar uma avaliação com falas livres, em uma palavra, ou disponibilizar uma filipeta com perguntas e pedir que os participantes respondam e entreguem no final. Enfim, existem várias possibilidades de avaliação, lembrando que a adaptação para o grupo e para o formato da atividade é essencial.

Avaliação de equipe:
A avaliação realizada pela equipe ocorre cotidianamente, geralmente no final das oficinas ou das atividades do dia. Ela serve como uma baliza para as próximas atividades. Expressam como as pessoas que estão mediando a atividade se sentem, qual é o clima do grupo e indica desafios e possibilidades para as atividades. É importante que neste momento as pessoas estejam atentas aos seus próprios processos de aprendizagem, mas principalmente ao processo dos participantes, evitando desentendimentos neste momento, e mantendo um clima de cumplicidade na equipe para que o processo, quando longo, ocorra da melhor maneira possível até a sua conclusão.

Nesse sentido, o cuidado com o processo é fundamental, e o roteiro de atividades auxilia bastante neste processo de revisão ou adaptação do que foi e está sendo feito. Com base nele podemos realizar as alterações que a equipe avaliar necessária sem perder a Guia sustentadora do processo.

Geralmente, em um processo de avaliação, dizemos coisas que marcaram a nossa presença nas atividades. Elementos que passam pela estrutura física, pelos conteúdos, pelas metodologias, mas também por aquilo que mais nos afetou. O que ficou da atividade. Por isso, se o processo de avaliação for bem conduzido e houver um bom ambiente, ele proporcionará uma boa aprendizagem e um bom re-planejamento de ações.

Muitas vezes esta avaliação não acontece logo ao término de uma oficina. Então, faz-se necessário um tempo de “decantação”, um tempo de “cair a ficha” dos conteúdos aprendidos. Neste caso, nós utilizamos questionários pós oficina, com perguntas bem abertas. Você também pode utilizar o próprio acompanhamento diário para avaliar ou medir os aprendizados!

Arthur Monteiro | @Congresso Nacional 2013

[pós-oficina]

Dúvidas, sugestões e como manter em contato são elementos que costumam surgir após uma oficina ou processo de aprendizagem em Segurança da Informação. Estabeleça um canal com as pessoas participantes para que o aprendizado continue, mesmo depois da oficina!

SUPORTE TÉCNICO

O processo de aprendizagem contínua por muito tempo depois da oficina, treinamento, palestra, etc. Logo depois do evento, há uma grande oportunidade para manter as pessoas interessadas em se atualizar e continuar a aprender, seja por meio de materiais ou outros tipos de contato. Na Segurança da Informação esse processo pode ser fortalecido de maneira digital.

Nosso aprendizado acontece principalmente quando temos exemplos sobre o conteúdo, troca de experiências, ou pessoas parceiras e facilitadoras que caminhem conosco. Por isso, uma forma eficaz de manter o grupo em contato é estabelecendo um canal para ele: crie uma lista de e-mails (veja o tópico *e-mail seguro*, em Recursos). A lista de e-mails pode servir a vários propósitos: pedidos de ajuda, compartilhamento de informações, discussões gerais e contações de histórias. Nessa lista, as pessoas facilitadoras têm um potencial muito grande como fomentadoras de informação e de discussão e, além disso, podem promover a interlocução e instigar a encontros online e offline (caso o grupo more na mesma cidade, por exemplo).

Como Suporte Técnico, que a pessoa que facilitou o encontro deve estar sempre atenta aos canais de comunicação que foram estabelecidos, para que quem pedir ajuda ou outro tipo de informação não fique a ver navios, mesmo que seja interessante que demais participantes do grupo também respondam às perguntas feitas. Lembre-se: sua opinião é muito importante para aqueles que receberam seu treinamento.

Outras boas maneiras de manter a produção de aprendizado viva são através de grupos de mensagens instantâneas. Nós recomendamos criar tais grupos em chats criptografados, como o *Signal*. Caso seu grupo de treinadores seja fixo e organizado, é possível criar outros canais de discussão, como: boletins de notícias, vídeos de treinamentos e histórias sobre o tema, páginas da internet, entre outras opções. De uma maneira ou outra, é muito importante que haja uma periodicidade mínima nas informações que circulam no grupo: mande notícias, atualizações na área de Segurança, pergunte como estão, se aprenderam algo novo, se têm dúvidas etc.

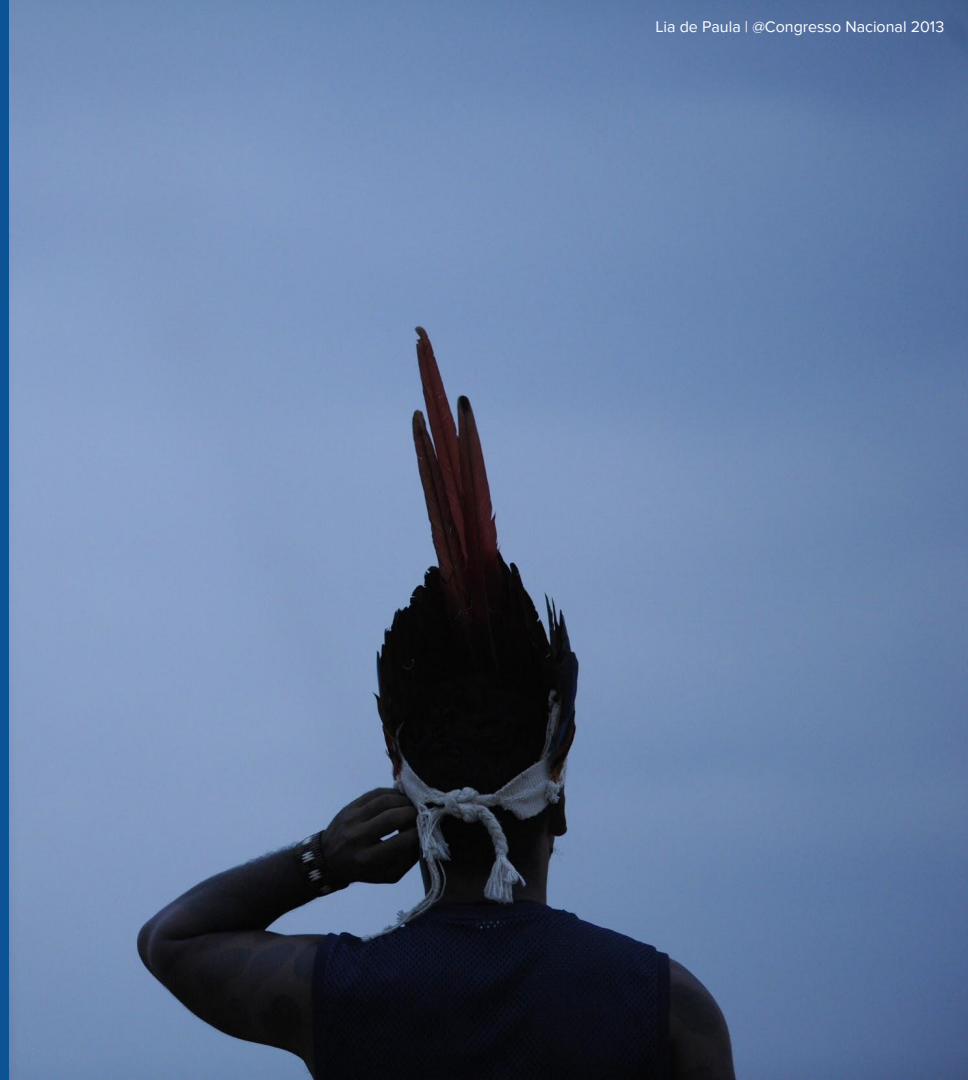
SUGESTÃO

Depois do evento é muito comum que as pessoas participantes venham até você e perguntem sobre onde buscar informações ou a quem recorrer quando tiverem dúvidas ou quiserem replicar o aprendizado obtido. Tenha essas respostas planejadas e, se possível, aja com antecedência: na sessão final de seu treinamento, pergunte qual o melhor canal de comunicação para um possível suporte ou para manter o grupo em contato: lista de e-mails, grupo em mensageiros instantâneos, apenas o e-mail das pessoas treinadoras disponíveis?

Nossa sugestão é criar uma lista de e-mails: assim, você mantém seu grupo unido, obtém um histórico das conversas no suporte e percebe se está indo no caminho certo para o aprendizado e treinamento coletivo. ▪

[conteúdo de apoio]

Nesta seção, convidamos pessoas que atuam na área de Segurança da Informação no Brasil para auxiliar na construção do contexto da vigilância e das ferramentas utilizadas no Brasil. Ela deve servir de base para realizar conexões com as ferramentas no momento da sua oficina. Lembre-se que esta área de conhecimento - como todas as outras - está sempre em mudança, e pode ser que alguns elementos já tenham se transformado quando você acessar este conteúdo, então, pesquise para manter seu aprendizado sempre atualizado.



Lia de Paula | @Congresso Nacional 2013

INTRODUÇÃO

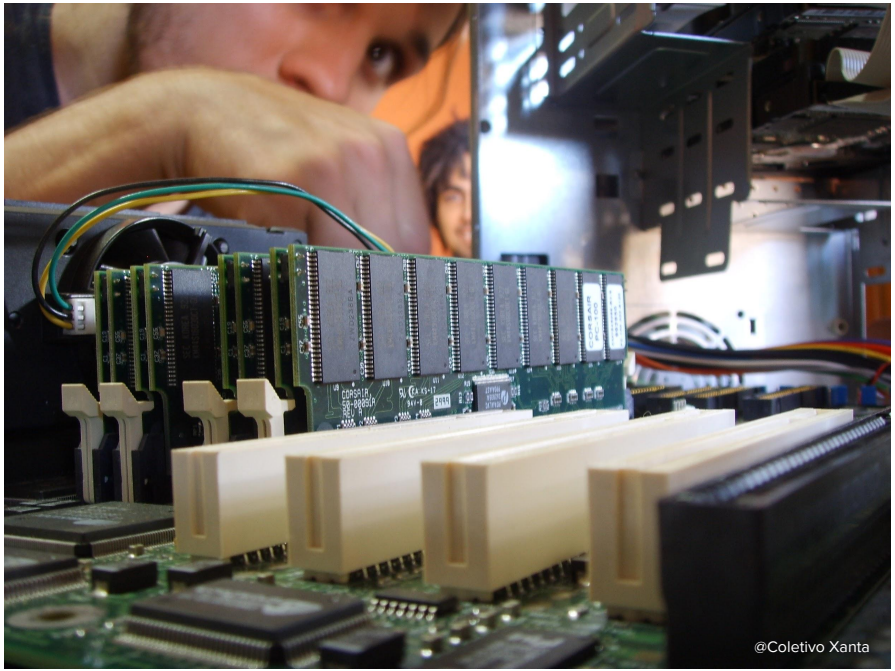
Além dos textos produzidos pelo Núcleo de Segurança da Informação da Escola de Ativismo, convidamos pessoas-chave para colaborar com este material, que aqui chamamos de Conteúdo de Apoio. São textos que apresentam contextos legais, técnicos e históricos da Internet no Brasil. Também damos atenção especial à Segurança Coletiva que ultrapassa as barreiras digitais, mas que impactam grupos ativistas de modo geral.

Estes textos estão assinados pois partiram de uma necessidade da Escola para produzir a Guia. Foram encomendados a pessoas que já pesquisam sobre o tema e portanto têm um acúmulo ou realizaram uma pesquisa específica para isso, por isso os créditos.

Mesmo que sejam textos de outras pessoas, convidamos você a interagir com o conteúdo, sugerir alterações e colaborar com essa produção. Para uma Guia mais completa e atual é interessante pesquisar mais artigos, variar as fontes, e ordenar os conteúdos aqui listados de acordo com as suas necessidades.

Os conteúdos do campo digital estão em constante processo, e portanto em constante atualização, nós consideramos importante que você tenha uma base de temas mais gerais para iniciar, mas que continue a escavação, a pesquisa, e sempre que possível faça contato conosco para que este material continue vivo. Nos envie um e-mail com suas atualizações para que possamos juntá-lo a este material online.

Boas leituras!



O ESTADO DA VIGILÂNCIA

Se, por um lado, as novas tecnologias de informação e comunicação trouxeram um potencial inovador para a organização de redes para ativistas, por outro, construiu-se uma teia de vigilância em massa sem precedentes. Hoje, a internet pode ser considerada uma ameaça global à privacidade.

Ao longo de muitos anos, os governos e as empresas implementaram secretamente - ou sem o devido escrutínio público - mecanismos de coleta e interceptação de dados. A doutrina de *ciberguerra* e a construção de *cibercomandos* pelos militares transformou a internet numa ferramenta de espionagem sem fronteiras. Dessa forma, a camada da infraestrutura global de comunicação e das novas tecnologias está comprometida.

Um dos mais recentes episódios de denúncia da vigilância global ocorreu em 2013, quando o então analista de inteligência da Agência de Segurança Nacional (NSA, em inglês) dos Estados Unidos, Edward Snowden, vazou milhares de documentos para uma equipe de jornalistas. Os documentos revelaram uma profunda teia de vigilância global de espionagem econômica e política realizada pela comunidade de inteligência do FVEY (Austrália, Canadá, Estados Unidos, Grã Bretanha e Nova Zelândia) contra diversos países, empresas com interesses econômicos conflitantes e até a Organização das Nações Unidas (ONU).

Sob a justificativa de proteger a sociedade contra “os cavaleiros do infoapocalipse” (terrorismo, tráfico de drogas, direito autoral e pedofilia), os governos e órgãos periféricos de vigilância, como as polícias forenses, também passaram a contratar serviços de empresas de *malware* e de *hacking* ofensivo. Uma vez que a comunicação do dia a dia passou a migrar para aplicativos, apenas a interceptação telefônica não seria mais suficiente para as investigações criminais.

Essas duas tendências de uso da rede por governos se reforçam, na medida em que a criação de uma estrutura de vigilância é justificada para proteger a sociedade contra um mal maior. Porém, essa estrutura de vigilância é, na verdade, utilizada de forma massiva e indiscriminada contra toda a população.

Embora o poder da vigilância global seja muito extenso, ainda assim é possível lutar contra ele. A chamada criptografia forte, ponto a ponto, é capaz de impedir que todos sejam vigiados. Ao utilizar aplicativos e ferramentas criptografadas, você não somente está protegendo a sua própria comunicação, mas também está lutando pelo direito coletivo de privacidade.

Além disso, é preciso realizar um debate intensivo com grupos, organizações e comunidade em geral na tentativa de abrir a temática da vigilância para encontrar possibilidades de abertura e mobilidade que incentivam uma política de pensamento que escape da condição de medo. Buscando uma nova mentalidade, ligada ao sentido da liberdade de agir e pensar na rede e no mundo. ▪

Por: Gustavo Gus

LEGISLAÇÃO E VIGILÂNCIA NO BRASIL

São três as principais leis que tratam das questões de monitoramento e vigilância no Brasil: Lei das Organizações Criminosas, Lei Antiterrorismo e Lei das Interceptações Telefônicas.

No Brasil, temos algumas leis que tratam de práticas de monitoramento tais como a interceptação das comunicações, o acesso a dados e a infiltração. Vale a pena destacar as seguintes:

Lei de Organizações Criminosas
(Lei Nº 12.850, de 2 de Agosto de 2013)

É uma lei de 2013 que altera o Código Penal e revoga a Lei nº 9.034/95, definindo o conceito de organização criminosa. A Lei dispõe sobre a investigação criminal e coloca como meios de obtenção da prova as seguintes práticas: colaboração premiada; captação ambiental de sinais eletromagnéticos, ópticos ou acústicos; ação controlada; acesso a registros de ligações telefônicas e telemáticas, a dados cadastrais constantes de bancos de dados públicos ou privados e a informações eleitorais ou comerciais; interceptação de comunicações telefônicas e telemáticas, nos termos da legislação específica; afastamento dos sigilos financeiro, bancário e fiscal, nos termos da legislação específica; infiltração, por policiais, em atividade de investigação; cooperação entre instituições e órgãos federais, distritais, estaduais e municipais na busca de provas e informações de interesse da investigação ou da instrução criminal.

A Lei de Organizações Criminosas é hoje um dos instrumentos mais poderosos para a vigilância e criminalização de movimentos sociais, grupos ativistas e dissidentes políticos. Em outubro de 2013, a Polícia Civil do Rio de Janeiro chegou a declarar, de acordo com matéria do jornal Estado de S. Paulo, que manifestantes detidos praticando atos de vandalismo seriam enquadrados na nova lei. Já em 2016, integrantes do MST passaram a ser investigados e dois chegaram a ser presos, com base na Lei, após denúncia do Ministério Público. Como desdobramento da mesma operação, em novembro de 2016, foram expedidos 14 mandados de prisão preventiva, outros 10 de busca e apreensão e ainda dois de condução coercitiva contra integrantes do movimento no Paraná, em Mato Grosso do Sul e em São Paulo. Na ocasião, a Escola Nacional Florestan Fernandes, importante centro de educação e formação da militância do MST, foi invadida por policiais armados, sem ordem judicial. Quando a Lei passa a ser utilizada como instrumento de criminalização, tais mecanismos se mostram ainda mais danosos. No caso do MST, ainda que a investigação esteja voltada a um grupo de pessoas, todo o Movimento pode estar sob vigilância, podendo ter, por exemplo, comunicações telefônicas e online interceptadas e agentes infiltrados.

Lei Antiterrorismo
(Lei nº 13.260, de março de 2016)

Outra lei preocupante em relação à sua utilização para criminalizar movimentos sociais é a Lei nº 13.260, que tipifica terrorismo. A Lei foi duramente criticada por parte da sociedade civil brasileira e, inclusive, pela Organização das Nações Unidas (ONU). As principais críticas dizem respeito ao caráter genérico do texto, que pode dar margem a interpretações distorcidas; ao fato de que a lei estipula penas muito severas; e ao fato de que as ações contidas na Lei já possuem tipificação legal no Brasil.

Em pronunciamento realizado em novembro de 2015, após o projeto ser aprovado no Senado, quatro relatores da ONU se disseram preocupados com a definição contida no texto, que poderia "resultar em ambiguidade e confusão na determinação do que o Estado considera como crime de terrorismo, potencialmente prejudicando o exercício dos direitos humanos e das liberdades fundamentais".

Lei de Interceptações Telefônicas
(Lei nº 9.296, de 24 de julho de 1996)

A intercepção de comunicações no Brasil é regulada pela Lei nº 9.296 / 96, que permite a intercepção nos sistemas de tecnologia de informação e telefone.

O objetivo estabelecido pela Lei é instruir procedimentos criminais ou investigações. O requisito é uma ordem judicial, que pode ser submetida diretamente por um tribunal ou solicitada pelas autoridades policiais e pelo Ministério Público.

Em linhas gerais, a Lei estipula que a interceptação só pode ser feita quando houver indícios razoáveis da autoria ou participação em infração penal, quando a prova não puder ser feita por outros meios, e quando o fato investigado for um crime punido com reclusão. Na prática, no entanto, esses pré-requisitos nem sempre são respeitados. De fato, o grampo é utilizado muitas vezes para iniciar uma investigação, como aponta o relatório final da CPI das Interceptações, de 2007: "A impressão desta Comissão é que as interceptações telefônicas transformaram-se, assim como a confissão no direito medieval, na "rainha das provas ", que torna a coisa notória, manifesta e inquestionável. Diante das facilidades tecnológicas atuais, interceptar as comunicações tornou-se uma alternativa tentadora, com certo menosprezo ao comando legal, no sentido de que deve ser esse o último meio de prova a ser usado". ▪

Fonte: Legado Vigilante, um projeto da Coding Rights

TÉCNICAS DE MONITORAMENTO

As principais técnicas de monitoramento utilizadas pelas polícias não são novas e sequer são as mais sofisticadas. Para se resguardar, são necessários alguns cuidados básicos de segurança operacional.

Em todas as democracias, os grupos ativistas são monitorados pela polícia. Não porque sejam considerados criminosos, mas por terem a capacidade de interromperem a ordem. Assim, não importando o quão juridicamente legal sejam a organização e as ações, qualquer grupo ou indivíduo que tenha como objetivo a mudança do *status quo* necessita tomar medidas de segurança. A segurança do grupo depende do compromisso de cada um. Por isso, é muito importante realizar processos de aprendizagem e acompanhamento nesse campo, seja coletivamente, seja individualmente.

O objetivo do monitoramento é coletar inteligência, isto é, ter dados chaves que possibilitem uma ação no futuro. Se antigamente a polícia necessitava colocar agentes para seguir os passos de ativistas e subversivos, hoje, com a internet, basta apenas um policial com a missão de fazer uma "ronda virtual" para navegar pelas redes sociais e ver quem são os responsáveis e articuladores de um determinado protesto.

Para evitar a ronda, é necessário tornar privadas, seja offline ou online, as ações estruturais do grupo, como reuniões, encontros, documentos e conversas de organização. É necessário avaliar e classificar quais são as informações sensíveis e quais são as informações públicas do grupo. Por exemplo, se uma determinada ação não-pública está sendo planejada, sua data de realização não deve constar nos documentos públicos do grupo.

Por exemplo, se uma determinada ação não-pública está sendo planejada, sua data de realização não deve constar nos documentos públicos do grupo. Embora muitos grupos tenham como princípio o livre fluxo de informação, a fim de evitar hierarquias ou desequilíbrio de poder, esse mesmo princípio não pode colocar seus membros em risco. Estabelecer um processo de controle de informações fortalecerá a sua organização à medida que os membros compreenderem quais são os riscos de um adversário ter posse de determinadas informações e do que eles estão abrindo mão ao não revelar uma determinada informação.

A outra técnica utilizada é descobrir como o grupo se organiza e quem são seus membros ativos. Isso pode ser feito por investigadores se passando por jornalistas, por exemplo. Portanto, ao dar entrevistas, não diga mais do que aquilo que já é ou será público. A rotatividade da figura pública pode ser muito útil e, além disso, um roteiro de perguntas e respostas prontas pode ajudar a limitar o acesso da mídia às informações do grupo. Também é importante, nas atividades públicas, existir rotatividade nas funções.

Por fim, caso se tornem um alvo, grampos e escutas telefônicas podem vir a ser utilizados. Ao evitar conversar por telefone sobre a organização ou, se precisar, utilizando criptografia ponta a ponta, a comunicação estará protegida. Fora isso, não há técnicas para impedir o grampo telefônico. E é por essa razão que ele é tão usado pelas autoridades policiais. ▪

Por: Gustavo Gus

MOBILIZAÇÃO E BOAS PRÁTICAS NAS REDES SOCIAIS

Usar as redes sociais como única ferramenta de mobilização social pode deixar sua organização fragilizada. Manter canais alternativos não só é saudável do ponto de vista da segurança, como também fortalecerá a luta.

Atualmente, diversas organizações passaram a centralizar a sua comunicação em sites de redes sociais como Facebook, Instagram e Twitter. Embora possam ter uma grande audiência na internet, rivalizando assim com a imprensa tradicional, do ponto de vista da Segurança da Informação, essas redes criam novos riscos que necessitam de atenção.

Um dos principais riscos ao mobilizar pelas redes sociais é a geração de grafos sociais que poderão ser utilizados para o mapeamento da sua organização e de seus apoiadores por um adversário. Se um observador externo é capaz de saber as funções, as pessoas responsáveis e o posicionamento político de cada um, ele será capaz de determinar as próximas decisões da sua organização e neutralizar as suas ações.

Além dos grafos sociais, ao concentrar a comunicação num único canal, cria-se um ponto único de falha, e, no caso das redes sociais, o risco é alto de ter a conta bloqueada ou invadida por atacantes, ou suspensa por políticas de moderação pouco transparentes. É também preocupante a ausência de preservação da informação, uma vez que toda a informação publicada pode não ser mais acessível no futuro pela sua organização. Portanto, além de uma boa política de senhas seguras e um controle de acesso a administração, você sempre deverá ter uma cópia das informações e também disponibilizá-las em outros canais: blogs, sites, outras redes sociais e a própria imprensa tradicional.

É necessário explorar e endossar alternativas de comunicação e incluir as redes sociais dentro de uma estratégia de comunicação. Além das redes sociais, quais outros canais de comunicação a sua organização está usando? E embora as redes sociais tenham uma grande audiência, ter pelo menos um mailing de suas apoiadoras e seus apoiadores será muito útil em diversas ocasiões. ▪

Por: Gustavo Gus

Romerito Pontes | @1º de Maio 2016

[introdução à segurança]

Para pensar Segurança, ampliamos nossos sentidos um pouco além da Informação, e sugerimos pensar o que essa palavra significa para cada pessoa. É um exercício pessoal, mas que nos ajuda a construir um conceito de segurança que possa ser ampliado e que faça sentido aos grupos ativistas das mais diversas áreas. Depois de refletir, abordamos questões diretamente ligadas à SI, como a própria Internet.

O QUE É SEGURANÇA

O Núcleo de Segurança da Informação da Escola de Ativismo vem realizando diversas atividades e estudos com a finalidade de aprimorar, renovar e construir outros modos de habitar a virtualidade, a internet, as redes sociais, de lidar com os meios de comunicação e com o sentido de vigilância cada vez mais difundidos no país e no mundo.

Nesta caminhada de inquietações e descobertas verificamos a necessidade de trabalhar com a palavra SEGURANÇA, descobrir o que havia dentro desta palavra-conceito e preenchê-la de significados novos, mais próximos daquilo que vínhamos pensando. Percebemos, então, uma imprescindível necessidade de sentir segurança no contemporâneo, algo como uma determinação para a vida ser possível na sociedade atual. Neste sentido, formulamos as seguintes perguntas problematizadoras: O que é segurança? O que é sentir segurança?

Em uma das atividades da Escola, essa pergunta trouxe respostas que nos provocaram:

- Sentir-se segura significa dançar livre em um salão...
- Quanto mais medo, menos potência. Quanto menos medo, mais potência.
- As soluções de segurança são produtos exigidos pela sociedade amedrontada. É a indústria da segurança e a produção do medo social.

Ao notarmos a complexidade e a profundidade destas perguntas, já que segurança pode ser um sentido, uma sensação, uma ação ou simplesmente a profissão de alguém que resguarda a vida de um conjunto de pessoas, percebemos que seria impossível e até mesmo pouco produtivo fazermos isso somente com o conjunto de pessoas da Escola. Decidimos, então, problematizar este conceito com os grupos que atuamos a partir da Escola de Ativismo ampliando, assim, as possibilidades de abertura para novos pensamentos a partir das perguntas e a abertura de possibilidades de mais e maiores interlocuções.

Um destes processos de abertura deste modo de pensar mais ampliado aconteceu na última residência em Segurança da Informação da Escola, um processo formativo que envolve grupos de diversos lugares do Brasil para o compartilhamento de saberes no campo da SI.

No primeiro dia do Encontro contamos um pouco deste percurso e então fizemos como descrito acima: lançamos as perguntas problematizadoras que tanto nos movimentaram, juntamente com a apresentação de cada pessoa que ali estava. O grupo tinha o apoio de algumas canetas e tarjetas para responder.

O grupo topou o desafio, e com estas perguntas puxaram diversas linhas. Para alguns, segurança lembrava o militarismo, tempos de um Brasil cheio de proibições e censuras em nome da Segurança Nacional, em favor da ordem e do progresso. Para outros, segurança lembrava liberdade, sentir-se à vontade com o próprio corpo e com os pensamentos. Teve gente que associou segurança ao medo. Medo como algo que paralisa, que retira a possibilidade de movimento, que interdita, interrompe, impede alguém de fazer algo.

E a segurança como algo inverso do medo. Houve também quem percebesse que a Segurança é um conceito em disputa e que existe todo um mercado de segurança que se organiza a partir do oferecimento de mais vigilância sobre os corpos. Também apareceu a segurança como algo importante para a sobrevivência, por isso ela também está atrelada à palavra alimentação - segurança alimentar.

Muitas palavras foram surgindo e se associando à palavra-conceito SEGURANÇA. Ao final da conversa, duas palavras apareceram com bastante intensidade: Controle e Limite. E a ideia de segurança pública que atua sempre nessa tensão entre controlar e limitar. O Estado como detentor do monopólio do uso da força permitida, e seus mecanismos como as polícias na atuação contra os movimentos no 'controle' de manifestações. Mas de onde vêm esses conceitos que são definidos juridicamente? ou mesmo o mercado, como no exemplo de uma empresa mundial como a google que, a propósito de organizar e armazenar dados, tem acesso às informações que permitem um controle sobre a vida contemporânea?

Essa atividade foi bastante interessante para nós. Pudemos explorar os pensamentos acerca da palavra Segurança e a quantidade de elementos que cabem dentro dela. Nosso intuito com esta sessão era justamente de, a partir desta palavra, descobrir possibilidades de atuação no sentido de oferecer mais potência e menos apreensão ou medo. Acreditamos que este propósito foi alcançado, já que o grupo embarcou nesta viagem conosco.

Outro aspecto importante foi abrir este conceito com um coletivo ampliado, um jeito de dizer que a Escola de Ativismo não estava conduzindo o processo de aprendizagem sozinha, mas que gostaria de fazer isso somando as concepções e opiniões neste campo de lutas ali reunido. O grupo mostrou muita disposição e a residência toda transcorreu nesse clima, nesse exercício de construção coletiva e, principalmente, de encontrar possibilidades e resistências nas lutas. ▪

Alguns textos que foram mencionados para saber mais sobre os assuntos:

Deleuze, Gilles. Post-scriptum sobre as sociedades de controle.

LECHNER, Norbert. Tem gente que morre de medo, 2015

Música:
Miedo, de Pedro Guerra / Lenine / Rodney Assis.

SEGURANÇA HOLÍSTICA E PSICOSSOCIAL

Buscando o "bem estar na ação", procura trazer mais consciência sobre segurança a partir de uma perspectiva de autocuidado e empoderamento pessoal e coletivo, baseada na percepção de nossos sentimentos e reações e em práticas de desenvolvimento de estratégias de segurança.

A segurança holística visa criar estratégias para manter o bem estar psicossocial das pessoas e criar espaços resilientes para ativismo e resistência, seja trabalhando individualmente, em coletivos ou em organizações.

Segurança é um conceito pessoal, subjetivo e variável de acordo com o gênero. Devemos levar em conta os efeitos de diversos tipos de violência, como violência física, estrutural, econômica, de gênero, institucional, assim como outros tipos de assédio e marginalização realizados por organizações privadas, grupos armados, pelos Estados e até pela própria comunidade ou pessoas próximas. Esses fatores afetam nossa saúde psicológica e física, nosso bem estar e nossos relacionamentos. Temos que estar alertas para identificar e implementar estratégias para a segurança e proteção de nós mesmos, das organizações de que fazemos parte e também das pessoas próximas.

A abordagem holística da segurança não trata somente do entendimento do papel da dimensão digital no âmbito pessoal e político, ou seja, das informações eletrônicas contidas em nossos dispositivos, bolsos, mochilas, casas, escritórios, ruas e veículos. Inclui também nossos corpos, emoções e estados físico e mental, promovendo uma cultura de cuidados e autocuidados como estratégia subversiva e política de auto preservação, construindo estratégias de segurança efetivas.

A abordagem proposta pode ser dividida em três níveis: segurança física, segurança digital e segurança psicossocial, que devem ser tratadas como questões integradas. As estratégias para lidar com essas questões devem ser constantemente revistas, da mesma forma que o contexto a nossa volta muda constantemente.

Algumas abordagens da segurança holística:

Resiliência e agilidade: Apesar da importância da implementação de planos estratégicos de segurança, situações inesperadas são comuns, e devemos estabelecer uma cultura de autocuidado, presença e equilíbrio mental e emocional para melhorar nossa capacidade de lidar com esses eventos. Assim, podemos cultivar resiliência para nos recuperar dos reveses e agilidade para rapidamente estabelecer novas práticas de segurança.

Trauma, stress e fadiga: Stress e fadiga podem nos levar a identificar e responder mal aos indicadores de ameaças no nosso meio ambiente. A sobrecarga resultante dos desafios em nossas casas, trabalhos e vidas e a fadiga gerada por trabalhar demais e por muito tempo sem descanso suficiente fazem com que tenhamos comportamentos diferentes.

O desenvolvimento de uma cultura (tanto individual quanto coletiva) de autocuidados e de administração do stress é fundamental para uma abordagem holística de segurança e bem estar.

Uso do tempo: O sucesso de uma prática de segurança depende do bom uso de nossos recursos, sendo o tempo um dos recursos mais valiosos a se considerar. Como indivíduos, precisamos de tempo para refletir sobre o efeito que nosso trabalho tem em cada um de nós, para elaborar perguntas e buscar respostas, para identificar táticas e ferramentas para planejar, coordenar e integrar novas práticas em nossas vidas e trabalho. Devemos conscientemente construir opções emocionalmente mais saudáveis e seguras quanto ao uso do nosso tempo.

Por: Foz

MOSAICO DE POSSIBILIDADES (MODELO DE AMEAÇA)

Somos diferentes, estamos em contextos diversos e as chances de estarmos em situações inseguras podem ser infinitas. O mosaico de possibilidades serve para traçarmos ações mais seguras em contextos específicos, sem entrar recairmos em paranoias ou inação diante da complexidade dos riscos, vulnerabilidades e possíveis defesas.

Chamamos essa atividade de "mosaico de possibilidades", pois ela envolve muitas peças, como ferramentas e procedimentos, que, juntas, formam um plano de possibilidades para ações seguras.

O início do mosaico exige, antes de tudo, que se prepare a base sobre a qual as peças serão montadas: o contexto. O contexto é algo externo e é aquilo em que não conseguimos interferir, como, por exemplo, a criminalização do ativismo. Ele nos mostra as ameaças existentes sobre uma situação ou grupo em um dado momento. É necessário compreendê-lo sob múltiplos ângulos: político, social, econômico, tecnológico e ambiental. A ferramenta que melhor atende a isso é a análise TEPAN (se preferir, chame-a de PASTEL), uma sigla que significa Política (P), Ambiental (A), Social (S), Tecnologia (T), Economia (E) e Legal (L). Você também pode inventar uma metodologia de acordo com a necessidade do seu grupo.

A partir daí, começamos a fazer uma série de mapeamentos para definir as vulnerabilidades, como:

1) Os recursos ou ativos: todas as pessoas, programas, aparelhos etc. que são essenciais para que o trabalho seja executado.
2) As atividades necessárias para que o grupo realize sua missão, como comunicar, organizar, fazer campanhas, etc.
3) As informações do grupo e onde estão armazenadas.

Por meio desses mapeamentos, analisamos onde estão os pontos fracos que tornam mais altos e prováveis os riscos provocados pelas ameaças.

Para analisar os riscos, é necessário posicioná-los segundo seu impacto (o quanto podem fazer mal) e sua probabilidade (as chances de acontecerem). Assim, saberemos quais riscos são mais prováveis e impactantes e, consequentemente, onde devemos focar nossas forças para melhorar nossas defesas.

CONTEXTO OU CASO

As ameaças podem ser diferentes de acordo com a situação política do país, a repressão sobre a causa que você defende, as tecnologias que estão sendo usadas para monitorar ativistas, e outros fatores.

Um exemplo: em um contexto onde há um governo opressor, e uma pessoa ativista jovem vai a uma manifestação, a ameaça é a criminalização do ativismo. Seu recurso é o celular, sua atividade é comunicar e suas informações são as articulações e contatos a respeito da manifestação que estão registradas num chat.

As vulnerabilidades possíveis são muitas: o celular pode não ter senha, a pessoa pode ser estudante, dentre outros aspectos.

Podemos definir alguns riscos: a pessoa pode ser atingida por uma bala de borracha; ser presa; ou ter o celular examinado por policiais.

E, analisando essas vulnerabilidades, chega-se à conclusão de que o risco de ter o celular apreendido é alto e que para diminuí-lo, é preciso construir possibilidades como colocar senha no celular, criptografá-lo e eliminar vestígios da articulação da manifestação.

SENHAS SEGURAS

Vários dos serviços seguros que permitem tornar nossas vidas menos expostas no ambiente digital irão requer uma senha. Em muitos casos, elas serão a sua última camada de proteção.

De um modo geral, quando queremos proteger alguma coisa, usamos uma chave para trancá-la. Travas de casas, automóveis e bicicletas, todas têm uma chave física. No ambiente digital, as SENHAS desempenham o mesmo papel: cartões de banco têm senhas, computadores têm senhas, contas de e-mail, ferramentas e etc.

Essas palavras secretas, frases ou sequências aleatórias costumam ser a primeira, às vezes a única, barreira entre a informação e alguém que possa querer lê-la, copiá-la, modificá-la ou destruí-la sem permissão.

Todas essas chaves, físicas e eletrônicas, possuem algo em comum: abrem os respectivos cadeados com a mesma eficácia independentemente de quem as esteja usando, você ou outra pessoa. Ou seja, se sua senha for fraca, ou se ela cair nas mãos erradas, não vai adiantar muito.

Existem vários meios que podem ser usados para descobrir senhas, mas é possível se defender da maioria com algumas táticas específicas e com o uso de uma ferramenta de banco de dados seguro de senhas, como o KeePassX.

A MINHA SENHA É SEGURA?

VOCÊ USA A MESMA SENHA EM MAIS DE UM SERVIÇO?

SIM

NÃO USE A MESMA SENHA EM MAIS DE UM SERVIÇO

SENHA INSEGURA

NÃO

É A SUA DATA DE NASCIMENTO OU DE ALGUÉM DA SUA FAMÍLIA?

SIM

NÃO

É UMA PALAVRA?

É UMA FRASE?

NÃO

SIM

NÃO

SIM

ESSA FRASE FAZ SENTIDO PARA ALGUÉM ALÉM DE VOCÊ?

SENHA INSEGURA

TEM CARACTERES ESPECIAIS?

NÃO

SIM

VOCÊ SABE A SUA SENHA DE CABEÇA?

SIM

NÃO

SENHA INSEGURA

VOCÊ USA UM GERENCIADOR DE SENHAS?

NÃO

SIM

SIM

NÃO

ESSA SENHA... É SEGURA????

verifique em **howsecureismypassword.net** *mas não digite sua senha real lá!*

VOCÊ É MAIS DO TIPO "RECUPERAR SENHA", NÉ?

COMO FUNCIONA A INTERNET

A infraestrutura da internet, os protocolos, tecnologias e intermediários por trás do tráfego de informações.

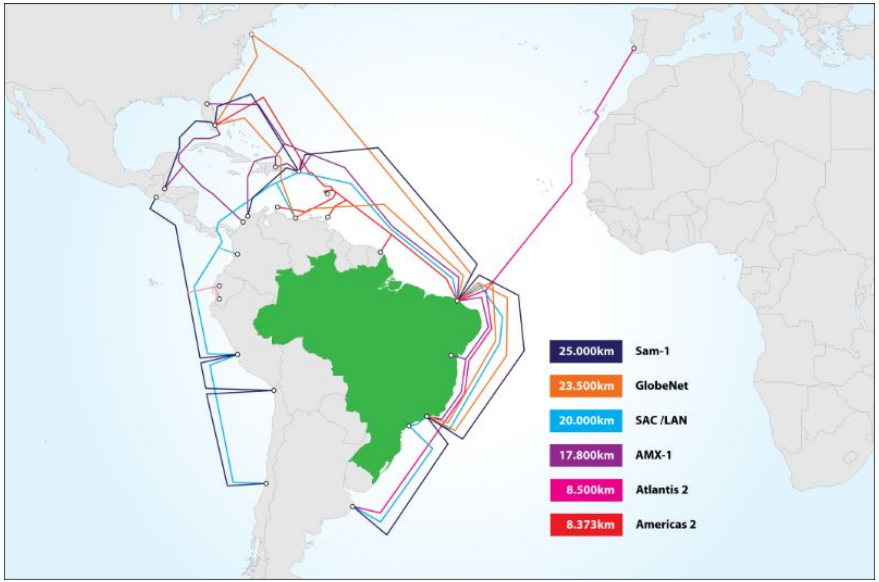
Muitas pessoas usam a Internet todos os dias, mesmo sem saber como ela funciona. Quando conversamos com nossas famílias pelo WhatsApp, enviamos e-mails para amigos e amigas e jogamos online, a Internet parece uma coisa mágica. E de fato é. Tecnologia é magia, e magia é tecnologia. Mas entender como essa mágica funciona é muito importante, e é uma questão política.

A Internet é uma rede de redes interconectadas. Daí o nome, inter, de interconectadas, e network, que significa rede em inglês. Internetwork! Ou simplesmente, Internet! Mas uma rede de quê? A Internet é uma rede de computadores (e pessoas!), que funciona de forma parecida a um serviço postal. Assim como o correio, que permite que você envie envelopes contendo mensagens e pacotes, a Internet permite que computadores se conectem entre si para enviar pequenos pacotes de dados contendo informações.

Quando pensamos na Internet, a primeira coisa que vem em mente é uma nuvem, certo? Ou uma imagem muito abstrata. Mas na verdade, a Internet é uma coisa bem física. Ela é feita, essencialmente, de cabos que passam por debaixo da terra (e do mar!), e conectam casas, países e continentes. Ao se conectar à Internet, você está se conectando a um cabo. É através dessa infraestrutura de cabos que nossos pequenos pacotes de dados vão trafegar, indo de um computador a outro. Para se conectar a uma página hospedada em um servidor nos Estados Unidos, por exemplo, os dados viajam pelos cabos, por debaixo do mar, até o outro continente e, em apenas alguns segundos, a página aparece na tela do computador.

Para se ter uma ideia, há, no mundo, hoje, mais de 360 cabos submarinos em funcionamento, que perfazem mais de 800 mil quilômetros — se juntássemos todos os cabos num só, eles dariam 20 voltas em torno da Terra. A história dos cabos submarinos é a história do capitalismo moderno. Desde as Grandes Navegações, europeus lançavam-se ao mar para fazer a roda do comércio girar e encurtar distâncias. Mas é em 1858, com o desenvolvimento industrial a pleno vapor, que começa a funcionar o primeiro cabo de comunicação transatlântico, construído pelos ingleses. Ele servia à tecnologia em voga à época: o telégrafo. Nos anos 1940, com o impulso da Segunda Guerra Mundial, os cabos submarinos foram convertidos para serem usados para telefonia. O domínio já não era dos britânicos, mas das empresas americanas. Nos anos 1980, por fim, surge a tecnologia da fibra ótica, que passa a ser usada nos cabos submarinos — muitas vezes seguindo as mesmas rotas traçadas no final do século 19.

Para que esse emaranhado de redes, cabos e dados funcione, a Internet é estruturada a partir de vários protocolos, como veremos a seguir:



Fonte: Francisco Jose Badaro Valente Neto
Cabos Ópticos Submarinos no Brasil - Uma abordagem conceitual

TCP/IP

Para que os computadores consigam se comunicar, eles utilizam uma "língua" comum chamada TCP/IP (Transmission Control Protocol / Internet Protocol). Todo dispositivo (computador, celular, tablet) conectado à rede recebe um número de IP, para que os dispositivos possam identificar uns aos outros. Para enviarmos uma carta para alguém através do correio, precisamos saber o endereço da pessoa. A mesma coisa acontece na Internet, então o IP é tipo um CEP, um identificador ou um endereço.

Cada página na Internet também possui um IP, para que possamos nos conectar a elas. Como números são muito difíceis de memorizar, foi criado um mecanismo para que possamos identificá-las e acessá-las através de endereços memorizáveis, ou seja, nomes. Se, por um lado, precisamos saber o endereço de uma página para nos conectarmos a ela, as páginas que acessamos também conseguem ver o endereço de IP que estamos usando. Passeamos de página em página deixando alguns rastros e um deles é o endereço de IP dos nossos dispositivos.

HTTP e HTTPS

Para acessar uma página, utilizamos também um protocolo de comunicação chamado HTTP (HyperText Transfer Protocol, que em português significa "Protocolo de Transferência de Hipertexto"), que é um conjunto de regras que permitem ao seu computador trocar informações com um servidor que abriga uma página. Isso significa que, uma vez conectados sob esse protocolo, os dispositivos podem receber e enviar qualquer conteúdo textual – os códigos que resultam na página acessada pelo navegador (chrome, firefox...).

O protocolo HTTP define, entre outras formalidades, como são requisitadas as páginas da Web, como são enviados os dados que uma pessoa insere em formulários de login e como o servidor envia mensagens de erro para o navegador de quem está acessando. No entanto, como o HTTP é um protocolo baseado em texto, ou seja, toda a informação transmitida está em texto, os dados de uma pessoa que usa a internet e do servidor podem ser interceptados ou alterados no meio do caminho.

Isso porque o HTTP foi desenvolvido para permitir a comunicação, e não a privacidade. Como hoje usamos a Internet para tudo, compartilhar informações, conversar com amigos e amigas, fazer compras e acessar nossa conta no banco, a privacidade se tornou uma das questões mais importantes.

Nesse sentido, um novo protocolo foi pensado e desenvolvido, o HTTPS. Ele insere uma camada de proteção na transmissão de dados entre seu computador e o servidor. Em páginas com endereço HTTPS, a comunicação é criptografada, aumentando significativamente a segurança dos dados.

É como se computador e servidor conversassem uma língua que só eles entendessem, dificultando a interceptação das informações.

Ao enviarmos um e-mail para uma pessoa, uma série de coisas acontecem: primeiro, conectamos nosso computador a um roteador através de uma conexão sem fio (wi-fi). O roteador, por sua vez, está conectado, através de um cabo, a um provedor de Internet (Oi, Net, GVT...), que nos concede a conexão à rede. Com o nosso computador conectado à Internet, o próximo passo é abrir um navegador (chrome, firefox) e acessar a página do nosso servidor de e-mail (Riseup, Gmail, Hotmail...). Lá, escrevemos o e-mail e enviamos ao servidor de e-mail da destinatária.

Se nosso computador estabelecer uma conexão com o servidor de e-mail através do protocolo HTTP, nossas informações irão trafegar pela rede sem nenhuma proteção. Seria como se estivéssemos enviando um cartão postal, e todas as pessoas que tivessem acesso a ele poderiam ler a mensagem. Por outro lado, se nosso computador estabelecer uma conexão HTTPS com o servidor de e-mail, nossa mensagem trafegaria com criptografia entre o computador e o servidor. Quem determina, em último caso, que protocolo será usado é o servidor, daí a importância de sempre prestar atenção se as páginas que visitamos usam HTTPS. Para isso, basta conferir, na barra de endereços do navegador, que protocolo está sendo usado.

O HTTPS também é importante para autenticar a página acessada. Ele contém um certificado que nos permite saber se a página que queremos acessar, por exemplo www.riseup.net, é realmente do coletivo Riseup. Isso dificulta que alguém crie uma página e tente se passar pelo Riseup.

VULNERABILIDADES NA INTERNET

A maneira como a Internet é estruturada hoje e a forma como a usamos tornam vários pontos da nossa conexão e navegação vulneráveis, e afetam nossa privacidade.

O roteador, o provedor de acesso à Internet e o provedor de serviço, por exemplo, guardam informações sobre nossa navegação. Desde o conteúdo do nosso e-mail, até o IP dos nossos dispositivos, o histórico das páginas visitadas, a data e hora que nos conectamos às páginas e à Internet etc.

Roteador:
Imagine duas pessoas com computadores conectados à internet na mesma casa. Uma delas atualizando seu perfil em uma rede social, outra trabalhando. O que impediria o tráfego de informações mobilizado por uma delas de serem enviados para outra? Duas coisas: os endereços de IP dos dispositivos, e o roteador. Roteadores direcionam o tráfego da Internet, ajudando os pacotes de dados a chegar no seu destino. Isso significa que toda a nossa navegação passa por ele.

Assim, quem possuir acesso ao roteador, pode ter acesso a informações de navegação de todos os dispositivos conectados a ele. É por isso que precisamos configurar os roteadores que usamos com senhas fortes e protocolos de segurança. É por isso também que acessar wi-fis públicos pode ser problemático: não é possível saber se há alguém farejando nossa navegação.

Uma forma de se precaver é prestar sempre atenção ao tipo de protocolo estabelecido para acessar as páginas. HTTPS é sempre mais recomendável que HTTP, e dificulta que terceiros conectados ao roteador tenham acesso a nossa navegação. Outra possibilidade é usar serviços e ferramentas como VPN (Virtual Private Network) e Tor.

Provedor de Internet:
Provedores de Internet são empresas que fornecem endereços de IP para acesso à Internet, como Oi, Net, GVT. De acordo com o Marco Civil da Internet, elas não podem bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados. No entanto, o Marco Civil obriga os provedores a coletar e armazenar logs de acesso à Internet, contendo o IP e a data e hora da conexão. Quer dizer, cada vez que acessamos a Internet, o provedor que contratamos registra a data e hora que conectamos e desconectamos, e o IP que utilizamos.

Página/Servidor de e-mail:
Visitar uma página é como visitar a casa de alguém: tudo que você faz por lá, a dona da casa pode ver. Além disso, todas as páginas que visitamos na Internet coletam e armazenam dados sobre nossa navegação e dispositivos. As pessoas que administram a página de um jornal, por exemplo, conseguem saber a que horas o IP do seu dispositivo visitou o site, em que links clicou, qual o sistema operacional do computador, que navegador está sendo usado, qual é o tamanho da tela, e muito mais, dependendo da política de privacidade da página.

Com essas informações, conseguem até traçar um perfil para as pessoas que visitam a página, mostrar publicidades direcionadas etc.

Já um servidor de e-mail comercial, como Gmail, Hotmail e Yahoo, além de coletar todas essas informações, também lê tudo que você escreve. Apesar de não cobrarem pelo uso, eles ganham dinheiro com os nossos dados, então vasculham e armazenam todos os e-mails, as fotos, os contatos. Sabem tudo sobre as pessoas que usam seus serviços, e podem vender esses dados para outras empresas, como as de publicidade, ou entregar esses dados para a polícia e agências de espionagem e Inteligência.

Para mitigar essa vulnerabilidade, não adianta utilizar HTTPS, já que o protocolo criptografa apenas a conexão entre nosso computador e a página. Isso significa que, para uma pessoa de fora, interceptar nossos e-mails pode ser uma tarefa difícil. No entanto, o conteúdo das nossas comunicações não está restrito aos remetentes e destinatários, mas também é acessado por quem provê o serviço. É como se o carteiro pudesse abrir e ler todas as cartas que enviamos.

Daí a importância de utilizar serviços de e-mail confiáveis e que se preocupam com a privacidade das pessoas. Serviços que não possuem como modelo de negócios os dados das pessoas usuárias, e que portanto não coletam informações sobre nossos dispositivos e não leem nossos e-mails, são bastante recomendáveis.

Nuvem

Quando você acessa uma página, você está na verdade conectando seu computador a outro computador, através de cabos e protocolos de comunicação.

Uma página é composta de arquivos, que “moram” em um servidor conectado à rede. Servidores não são nuvens que pairam no ar, mas computadores, ligados à energia, e localizados em algum lugar do mundo. Então quando alguém fala de nuvem, tá falando, na verdade, de um computador. A nuvem é sempre o computador de outra pessoa.

A INTERNET QUE QUEREMOS

Já sabemos Como a Internet Funciona, e temos bastante conteúdo para construir a nossa própria internet, como com as Redes Mesh. Tendo em vista nosso conteúdo e nossos desejos, **qual é a Internet que queremos?**

Podemos pensar que a Internet é um espaço maravilhoso, estranho e muito diverso, com milhões de vozes, perspectivas e motivações que se diferem e se transformam todos os dias. Com isso, existem várias ferramentas e vários pontos que podemos analisar e trabalhar para construir a nossa própria Internet, mais inclusiva, segura e lúdica.

Trazemos aqui algumas perguntas que podem inspirar você para pensar a Internet que você e/ou seu grupo quer:

- A Internet é aberta? Quais são os direitos e deveres que as pessoas, as empresas e os governos têm sobre ela? Há censura? Os programas são abertos e acessíveis?
- A Internet é livre? Todas as pessoas podem se conectar pela internet com boa banda larga e velocidade? A linguagem da Internet é acessível para todas as pessoas? Há segurança?
- Quem comanda e manda na Internet? Quais são as leis e quais são as regulamentações que você e/ou seu grupo gostariam que existissem na internet? Nessas legislações, como atuam as grandes empresas, os governos, as pequenas comunidades?
- Eu sinto segurança quando utilizo a Internet? Quais são os riscos e as vulnerabilidades que a vida na web me proporciona? Na Internet que você quer, como seria a segurança?
- Há padrões na Internet dos sonhos? Todas as pessoas sabem do que se trata e conseguem manipulá-la à primeira vista? Como funciona a educação na Internet que queremos? Quais são as ferramentas de aprendizagem ativa que existem nela?
- Que pessoas são bem-vindas na Internet que queremos?
- Quem controla a Internet que queremos?

Saiba mais sobre a saúde da internet.

Esses pontos são só para você se inspirar, existem muitos outros que podem povoar o imaginário da internet: como o próprio ativismo em si (uma Internet Feminista, Anarquista, Ambientalista, Indígena, Quilombola, entre muitas outras). O que propomos aqui é que você e seu grupo façam um exercício de imaginação e criatividade, explorando os sentidos, os desejos e as possibilidades de uma nova Internet. Não tenha medo de cruzar fronteiras, pois já dizia um velho pensador: não sabendo que era impossível, foi lá e fez!

Desenhe, rabisque, inspire-se!

COMO FUNCIONA O TELEFONE CELULAR

A estrutura do aparelho telefônico, a infraestrutura da rede telefônica e suas vulnerabilidades.

Eles são a última coisa que olhamos antes de ir dormir e a primeira que tocamos ao acordar. Os smartphones mudaram a nossa maneira de nos comunicar e também criaram vulnerabilidades que lhes são próprias. Da infraestrutura às conexões virtuais, o telefone e o smartphone podem potencializar nossas vozes ou calá-las.

Os dispositivos móveis possuem muitos sensores e funções e nossa maneira de gerenciá-los transforma a segurança de nossas informações. O número de funções disponíveis nos telefones celulares cresceu nos últimos anos, e os aparelhos modernos são, na verdade, mini-computadores portáteis, conectados à internet com características de telefone celular, que podem incluir localização/GPS, geração e transmissão de arquivos multimídia (gravação e transmissão de foto, vídeo e áudio), processamento de dados e acesso à internet, além do tradicional envio de SMS e ligações telefônicas via operadora.

É importante compreender que telefones celulares são inerentemente inseguros:

> As informações enviadas e armazenadas nos telefones ficam expostas (armazenadas sem criptografia) nos aparelhos de origem e de destino das comunicações.

> Para viabilizar a cobrança do serviço, o sistema é projetado para expor informações sobre sua localização (em que antena o dispositivo está conectado), e os metadados das suas comunicações (quem falou com quem em que hora).

> A informação sobre a localização (incluindo a localização GPS) pode estar embutida em outros arquivos como fotos, mensagens SMS e requisições de internet enviadas pelo telefone.

> As redes de telefonia celular são privadas e geridas por entidades comerciais, e podem estar sob o controle do governo, por diversos motivos (legislação, espionagem, etc).

> Os Sistemas Operacionais usados nos próprios dispositivos móveis são desenvolvidos sob medida ou configurados pelos fabricantes de aparelhos telefônicos, segundo as especificações de vários provedores de serviços e para serem usados nas redes dessas mesmas empresas. Como resultado, o Sistema Operacional pode ter funções escondidas para possibilitar um melhor monitoramento por parte do provedor de serviços de determinado aparelho.

Por isso, é importante tomar decisões conscientes ao usar telefones celulares para que possamos nos proteger, proteger as pessoas com as quais nos comunicamos e nossas informações. O modo como as redes e a infraestrutura de telefonia funcionam pode afetar de forma significativa a possibilidade de manter os dados e as comunicações privados e seguros.

A estrutura básica do celular é a seguinte:

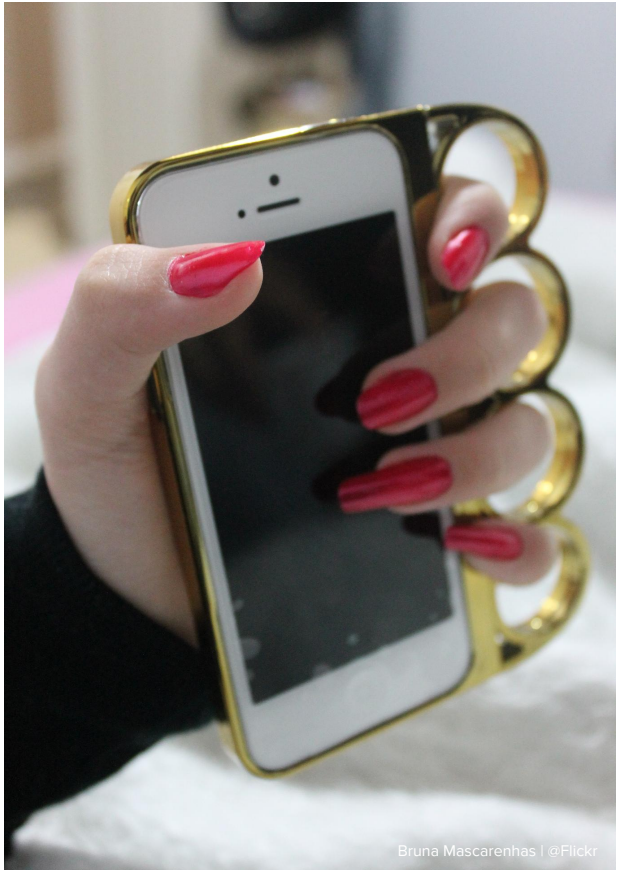
Hardware
É a combinação das peças físicas do aparelho.

Firmware
São softwares de base - ou seja, que atuam diretamente no hardware, ao invés do sistema operacional.

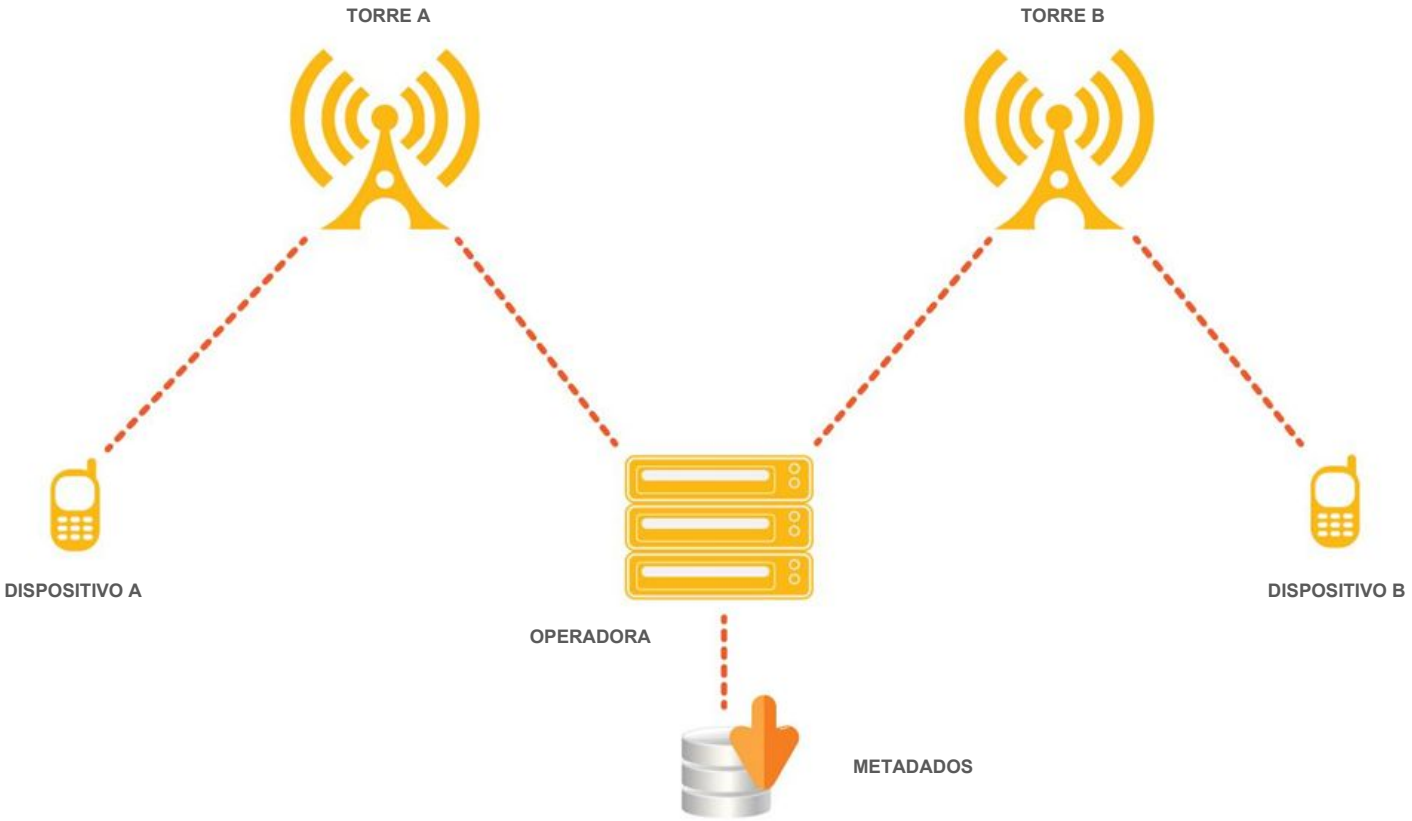
Bootloader
Conjunto de sistemas que permitem a inicialização do aparelho; cada dispositivo tem seu próprio bootloader.

Modem
Componente proprietário essencial para a utilização das funções de telefonia móvel.

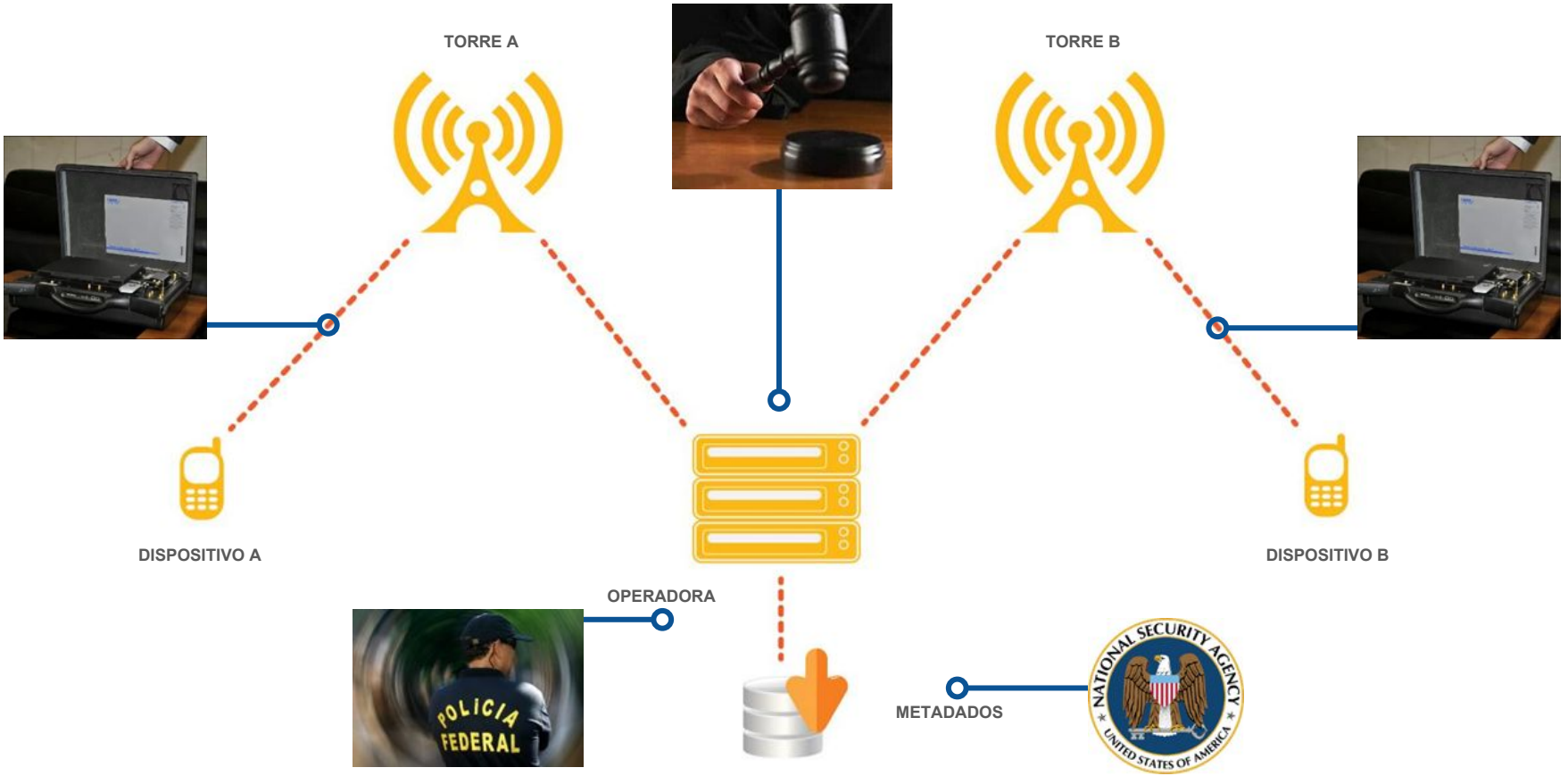
Sistema Operacional
É o sistema operacional que vem no celular, ou seja, pode ser Android, iOS, Windows, Ubuntu, entre outros.



INFRAESTRUTURA BÁSICA DA REDE TELEFÔNICA



VULNERABILIDADES DA REDE TELEFÔNICA



[ameaças]

Apresentamos um conjunto de ferramentas e ações utilizadas por governos, empresas e pessoas ou grupos que tentam rastrear e vigiar dados e atividades de quem quer que seja - ativista ou não - na Internet, nas comunicações telefônicas e até mesmo em manifestações.

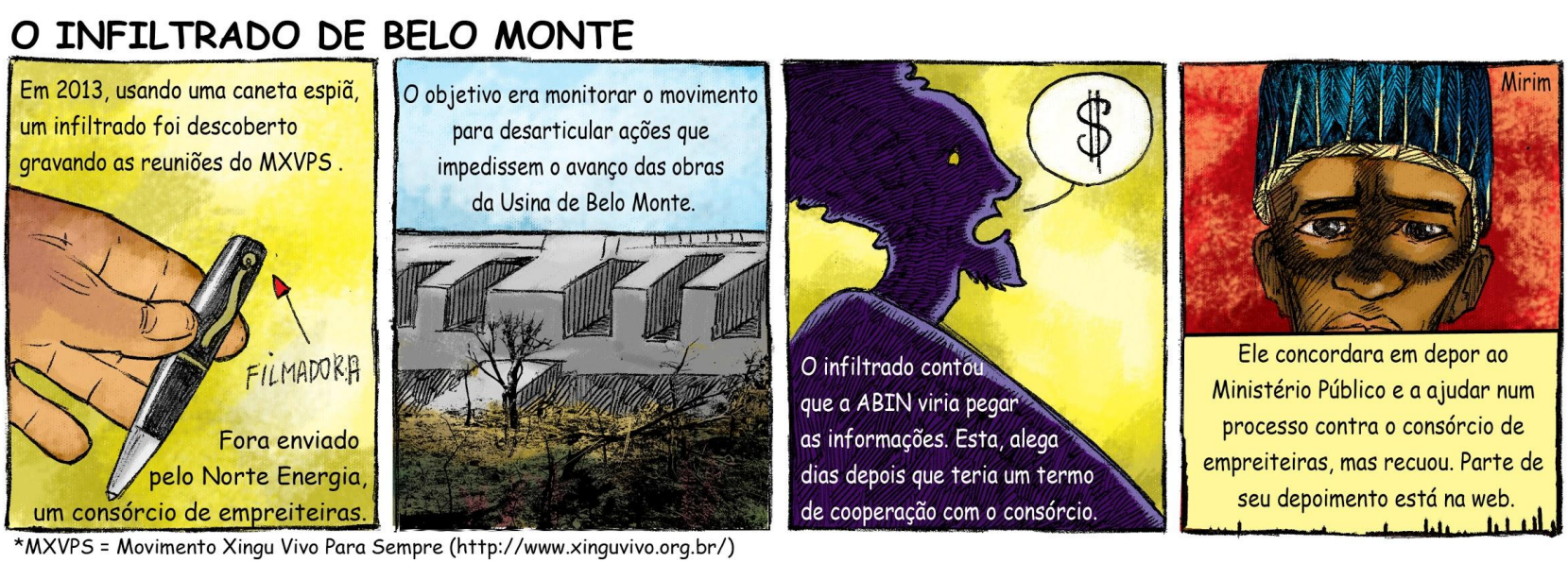
Marianna Cartaxo | Mídia Ninja

ENCONTRE O P2: **P2** é uma categoria do serviço da inteligência da polícia que também pode ser chamado de **serviço reservado**. Esse policiais andam disfarçados e podem estar inseridos nas manifestações, faculdades, bares e festinhas do movimento. Se liga!

Ilustração: Mirim

INFILTRAÇÃO: Com o uso de identidades falsas ou através da corrupção de pessoas envolvidas, agentes de governos ou de empresas procuram entrar em grupos ativistas como se fossem integrantes das mesmas, acompanhando suas atividades e conhecendo sua estrutura, para que criar estratégias que, em grande parte das vezes, resulta na dispersão e desmobilização das atividades dos grupos.

Ilustração: Mirim



*MXVPS = Movimento Xingu Vivo Para Sempre (http://www.xinguvivo.org.br/)

GRAMPO

COMO FUNCIONA?

A interceptação da comunicação, interceptação telemática ou, mais genericamente, o grampo, é a gravação da comunicação entre duas ou mais partes por um atacante. Há diversas formas de se grampear uma conversa, seja com gravadores acoplados ao corpo até a interceptação nas empresas de telecomunicação. O grampo pode ser um equipamento simples, de baixo custo, como um gravador, empregado tanto por detetives particulares e grampeiros, quanto patrocinado pelo Estado. Para além de grampo do telefone, conversas em aplicativos também podem ser interceptadas. No Brasil, o grampo é o principal instrumento de investigação e, embora tenha uma legislação específica, ela não limitou o seu uso massivo, pelo contrário, ampliou a colaboração entre Estado e empresas de telecomunicação. Ainda no modelo de ameaça do grampo, é necessário levar em consideração que o atacante pode ser a própria parte envolvida na comunicação.

COMO SE PROTEGER?

Adote a seguinte premissa de Segurança da Informação: se não está criptografado, então está grampeado. No telefone, não utilize códigos como substituição de palavras ou palavras/frases chaves, elas são triviais para serem desvendadas por investigadores. Opte por falar assuntos sensíveis pessoalmente ao invés de utilizar meios digitais. Embora existam equipamentos telefônicos criptografados, eles são caros e todos os envolvidos na comunicação precisam ter um. Uma solução mais adequada é utilizar softwares de chamadas telefônicas com criptografia ponto a ponto, como o Signal, e checar a identidade do seu colega pessoalmente.

REFERÊNCIAS

Grampolândia - A república da escuta: https://grampo.org

Por: Gustavo Gus

RONDA VIRTUAL

COMO FUNCIONA?

Imagine o guarda de ronda de um bairro, sempre à espreita de um acontecimento não usual. A ronda virtual é como a ronda do bairro, mas acontece no ambiente virtual e especialmente nas redes sociais. Mas também existem empresas que prestam esse serviço a empresas, políticos, etc. Como funciona? É, literalmente, uma pessoa observando TUDO que você publica nas redes sociais, o que você curte, compartilha, os eventos a que você decide ir, entre outras atividades.

Há alguns casos de ativistas que foram presos, durante cenários políticos específicos, com o apoio de investigações policiais que utilizam esta técnica de monitoramento. Um desses casos ocorreu entre 2013 e 2014, no Rio de Janeiro, conforme descrito em inquérito policial que levou à prisão de pelo menos 20 ativistas. Com uso da ronda virtual, policiais monitoraram redes sociais e definiram quem era suspeito com base em postagens, comentários, fotos, tags e redes de amizade no Facebook.

COMO SE PROTEGER?

Uma das melhores maneiras de se proteger da ronda virtual é se atentar para as configurações de privacidade e restringir ao máximo o acesso ao seu perfil e aos seus dados (veja mais na seção “Redes Sociais mais seguras”), especialmente os das redes sociais.

Também é uma boa prática utilizar perfis diferentes para interações e ações específicas nas redes. Por exemplo, é possível utilizar um perfil para interações mais pessoais, com pessoas amigas e familiares, e outro perfil para ações como a administração de páginas ou para fazer denúncias. O perfil mais pessoal pode ser configurado para priorizar a privacidade, enquanto o outro perfil pode ser utilizado com um pseudônimo e registrado com um email que não seja pessoal. Também é recomendável usar a rede Tor ou VPN para acessar esse perfil, de modo a não revelar seu IP. Utilizar perfis com pseudônimos e acessados via Tor pode causar problemas com o Facebook, que tende a questionar e apagá-los. No entanto, é importante insistir.

Mais sobre o assunto em:
> Mobilização e boas práticas nas Redes Sociais
> *Redes Sociais mais seguras*
> *Navegador Tor*
> *VPN*

REFERÊNCIAS

Vigilância das Comunicações pelo Estado Brasileiro.

RASTROS DIGITAIS - METADADOS

COMO FUNCIONA?

Nós geramos metadados sem saber, de uma maneira ordenada e durante um longo prazo. Eles são as informações que acompanham seu e-mail, sua mensagem, suas imagens/fotografias ou algum outro comportamento seu na internet; podem ser informações de geolocalização, data e hora, quem executou (o arquivo, a fotografia, o aplicativo). E, além disso, os metadados deixam mais fácil a análise, o reconhecimento de padrões e as conclusões sobre quem somos e o que estamos fazendo.

As empresas que estão no centro de nossas comunicações – como os provedores de telefonia celular ou de serviço de internet ou de e-mail – têm registros detalhados desses metadados e isso dá a elas, e a qualquer um que tenha acesso a essas informações, um retrato muito preciso das pessoas que produzem esses rastros digitais.

COMO SE PROTEGER?

Tenha controle sobre seus dispositivos, veja:
> Como funciona a Internet
> Como funciona o Telefone Celular
> Programas Anti-Metadados

REFERÊNCIAS

Rastros Digitais

BACKDOORS

COMO FUNCIONA?

Os protocolos técnicos que compõem a Internet utilizam o conceito de portas para organizar a comunicação entre os diferentes serviços da rede. Cada serviço pode receber conexões em uma ou mais portas de entrada. *Backdoors* (ou "portas dos fundos" em inglês) são portas de entrada em algum programa que possibilitam acesso a um sistema sem que o usuário ou administrador saiba ou tenha controle.

Estas portas dos fundos podem ser abertas por ataques a falhas de segurança de um programa ou sistema operacional. Nestes casos é comum que, durante o ataque, sejam instalados outros programas (muitas vezes escondidos ou disfarçados de outra coisa) que podem chegar a dar à pessoa atacante acesso total ao computador atacado.

Em outros casos, a porta dos fundos é instalada deliberadamente, às vezes até por força de lei (veja abaixo o link para a história do *Chip Clipper*).

É bastante comum que os *backdoors* resultem em acesso total ao software e hardware do computador atacado, incluindo dados armazenados, webcam e dispositivos de USB e DVD, entre outros.

COMO SE PROTEGER?

Os *backdoors* podem ser instalados em um computador por meio da execução de anexos de e-mail infectados ou programas baixados de sites maliciosos que carregam vírus. Algumas maneiras de se proteger desse tipo de ataque são:

> Não executar programas baixados de sites desconhecidos, nem anexos de e-mails suspeitos.

> Sempre usar um antivírus e sempre mantê-lo atualizado.

> Usar um *firewall* no computador funciona como uma barreira de conexões e pode impedir um atacante de se conectar com um *malware* já instalado.

REFERÊNCIAS

Chip Clipper

Guia de Autodefesa Digital - Computadores

Security in a Box - Como proteger seu computador de ataques maliciosos e hackers

MALWARE

COMO FUNCIONA?

Malware é uma junção das palavras em inglês *malicious software* ou, em português, *programa malicioso.* É uma forma de se referir à imensa gama de diversos tipos de programas maliciosos que existem na web: vírus, *spyware*, *phishing*, *trojan*, etc. Um *malware*, por definição, sempre tem algum objetivo escuso. Os ataques podem pretender roubar dados pessoais, senhas, dados bancários, informações sensíveis, entre outros.

Um *malware* pode não estar sendo executado em seu computador e mesmo assim causar danos. Nos ataques chamados de *phishing*, por exemplo, um website falso (em um servidor malicioso) pode imitar o Facebook, ou uma página de um banco, ou e-mail, ou qualquer outro site que pessoa esteja acostumada a frequentar, e assim roubar seus dados de acesso.

Em outros casos (como os vírus/*spyware*/*adware*) o programa malicioso roda no próprio computador da pessoa, e a infecção pode acontecer através de um programa recebido em algum HD externo ou pendrive infectados, ou de algum programa baixado ou anexo mal-intencionado recebido.

COMO SE PROTEGER?

O quanto estamos suscetíveis a programas maliciosos depende da maneira como nos comportamos como indivíduos na web e como usamos nossos dispositivos:

> Não abra e-mails e arquivos de pessoas que você não conhece, principalmente se o assunto do e-mail for genérico como "As fotos da festa ficaram ótimas";

> Não use pen-drive e outros dispositivos usb de pessoas estranhas, e sempre passe um antivírus;

> Mantenha seu computador, seu antivírus e outros programas de precaução sempre atualizados;

> Verifique sempre se o endereço do site que você está acessando é o verdadeiro;

> Não clique em links suspeitos.

BIOMETRIA

COMO FUNCIONA?

Biometria é a identificação e/ou autenticação de uma pessoa baseada em características biológicas únicas, tais como a geometria da voz, da escrita, da impressão digital, da íris, da orelha, da face ou da mão. Por ser uma nova tecnologia, ela se propõe a uma autenticação mais segura. Porém, apresenta problemas até maiores do que outras autenticações, como vazamento e roubo de impressão digital e outras características pessoais. Além disso, se você usa essa tecnologia em seus dispositivos, tais como celulares ou tablets, uma vez apreendidos ou roubados, seus dados ficarão disponíveis para a autoridade que o capturou.

Um exemplo da diferença da biometria para as outras maneiras de identificação é a senha, que uma vez criada, você a mantém privada. Além disso, você provavelmente mantém o número do seu cartão de crédito privado também, no entanto, na biometria qualquer pessoa pode olhar para você e ver sua íris ou pegar sua impressão digital de algo que você tocar. Sua face e suas impressões digitais podem já estar, inclusive, em poder dos bancos de dados de autoridades. E uma vez que você estiver em território público, qualquer pessoa pode tirar sua fotografia.

COMO SE PROTEGER?

Em caso de perda de senhas ou de hackeamento de suas contas com elas, o que você precisa fazer? Mudar ou recuperar sua senha, ou no caso de perda de cartão de banco, cancelá-lo. Mas se fizerem isso com a sua impressão digital, dificilmente será possível mudá-la. Por isso, a principal recomendação é não usar a biometria como sua autenticação primária, pois você não pode mudá-la.

MAN-IN-THE-MIDDLE

COMO FUNCIONA?

Man-in-the-middle significa, em português, “homem no meio”, e é um tipo de ataque no qual o atacante consegue se posicionar entre as duas partes que estão se comunicando e interceptar a comunicação. Para poder fazer esta interceptação, o atacante precisa conseguir uma posição estratégica em alguma rede ou programa que participe da comunicação. Uma vez interceptada a comunicação, o atacante funciona como um intermediário, se passando por cada uma das partes na comunicação com a outra. Um exemplo comum é o de contas e faturas falsas na internet.

Uma forma comum de *man-in-the-middle* é o uso de um *malware* que “sequestra” seu navegador de internet e passa a ter acesso às informações que você envia ou recebe através dele. Outra forma comum é a exploração de vulnerabilidades em roteadores sem fio e a interceptação das informações transmitidas por ele. Este tipo de prática tem resultados mais graves pois atinge mais pessoas, ainda mais quando se tratam de roteadores públicos, como de cafés, metrôs, hotéis, etc.

COMO SE PROTEGER?

*> Utilize sempre conexão criptografada (com o **S** de HTTP**S**), especialmente para websites em que você precise colocar seu login e senha. Essa tecnologia de criptografia tem como objetivo proteger os dados que trafegam e também autenticar o site com o qual você está se conectando.*
Use a extensão HTTPS Everywhere:
https://addons.mozilla.org/pt-BR/firefox/addon/https-everywhere/
https://chrome.google.com/webstore/detail/https-everywhere/

> Mantenha seus navegadores e computadores atualizados;

> Utilize autenticação de dois fatores nos websites que você mais frequenta (como redes sociais) e celulares;

> Não clique em links dos quais você desconfia, especialmente aqueles que vêm em e-mails cuja pessoa remetente você não conhece.

HACKING - ATAQUE INTENCIONAL

COMO FUNCIONA?

Os ataques intencionais de hackers podem acontecer de várias maneiras: uma pessoa mal-intencionada que está à sua volta, um/a parente querendo descobrir mais coisas de sua vida, um hacker que quer roubar você ou ataques aleatórios de hackers com uso de vários tipos de vírus, como o WannaCry. Esses ataques podem acontecer de várias maneiras: através de Malwares, Man-in-the-middle ou até mesmo roubo.

COMO SE PROTEGER?

Existem várias maneiras de manter seus dados e dispositivos mais seguros, mas a melhor maneira é uma combinação de comportamentos seguros.

Para começar, recomendamos que use um sistema operacional livre, como o GNU/Linux, que sofre menos com ataques de *hacking* do que os fechados. Além disso, mantenha seus programas sempre atualizados, especialmente se forem atualizações de segurança; também é necessário implementar e manter senhas seguras:

> senha de login
> senha de administração de sistema
> senha de bloqueio de tela

Se possível, use um gerador de senhas para ter senhas mais seguras, como o KeepassX. Caso você precise usar sistemas fechados, como o Windows, atente-se sempre para o uso e atualização de antivírus, antispyware e bloqueadores de anúncios (recomendamos o uso do *uBlock Origin*). Ou seja, um conjunto de comportamentos, que mitigam perda de dados, mantém seus dispositivos seguros e seus backups atualizados.

PERDA, ROUBO, APREENSÃO OU ACESSO JUDICIAL

COMO FUNCIONA?

Uma distração num café, um *happy hour* com a galera da firma, uma chuva no caminho de volta para casa à pé ou de bicicleta, além de outros fatores, podem nos levar a perder nossos dispositivos eletrônicos e digitais que mais usamos. Seja uma perda acidental ou intencional (roubo ou apreensão), ela pode nos levar a ficar sem nossos equipamentos e, principalmente, sem nossas informações mais preciosas. Além disso, ela também pode tornar outras pessoas vulneráveis - amigos, família, trabalho ou coletivo ativista. Por isso, algumas medidas são importantes para manter os dispositivos seguros.

COMO SE PROTEGER?

Uma combinação de atitudes e comportamentos gerais pode garantir que você terá seus dados seguros e disponíveis para você.

> Backup criptografado e atualizado;
> Senhas seguras;

No caso de uma apreensão judicial, em que, provavelmente, você terá todos seus equipamentos apreendidos, recomendamos que tenha o computador criptografado e, possivelmente, um backup em uma nuvem ou em outro local seguro, também criptografado.

REFERÊNCIAS

Senhas seguras

Security in a Box Como proteger seus dados de ameaças físicas

Rosilene Miliotti | FASE

[recursos]

Nesta seção, trazemos ações e ferramentas para manter sua vida digital mais segura. Lembre-se sempre de pesquisar e atualizar as informações que disponibilizamos aqui.

PROGRAMAS ANTI-METADADOS

COMO FUNCIONA?

Metadados são informações de um arquivo (como um documento de texto, um PDF, uma imagem, um arquivo de música etc.) que são armazenados no próprio arquivo. Essas informações podem incluir a hora e data em que o arquivo foi criado, o nome de usuário das pessoas que o criaram ou editaram, informações sobre o dispositivo que o criou e outros tipos de informações, como a geolocalização. Como resultado, os metadados em um arquivo podem dizer quem criou um arquivo, em qual computador ou dispositivo, quando e em que localidade. Os programas Anti-Metadados, basicamente, removem todas as informações (ou informações selecionadas) de um determinado arquivo.

COMO SE PROTEGER?

Você pode verificar os metadados de uma foto clicando com o botão direito do mouse sobre ela e selecionando Propriedades ou usando um software de visualizador de metadados, como o Photome. Além disso, é possível evitar que um tipo específico de metadados, como localização GPS, seja capturado:

> Desligue localização wireless e GPS (em serviços de localização) e dados móveis (isto pode ser encontrado no gerenciador de dados -> entrega de dados).

> Ao tirar uma foto, certifique-se de que as configurações da localização da tag do app de fotos também estão desabilitadas.

Se você quiser remover o metadado de vários arquivos, você pode usar programas específicos como Metanull (remove metadados de imagens, no Windows) ou o MAT, que remove metadados de vários tipos de arquivos.

REFERÊNCIAS

Removendo metadados (inglês)

Programa anti-metadados do linux - MAT

NAVEGADOR TOR

O QUE É?

O Navegador Tor é um programa de software livre e código aberto, arquitetado para possibilitar o anonimato online e para burlar a censura. Ele funciona numa grande rede de milhares de servidores, administrados por pessoas voluntárias em todo o mundo. Para fazer uma nova conexão, ele seleciona três desses servidores, chamados de transmissões Tor, e se conecta na Internet através delas. Ele criptografa cada parte desse trajeto, de modo que eles não saibam para onde os dados são enviados e recebidos.

Ao usar o Navegador Tor, o seu tráfego na internet aparentará vir de um endereço IP diferente, geralmente de um outro país. Consequentemente, o Navegador Tor torna seu endereço IP oculto dos sites que você acessa, bem como oculta tais acessos a terceiros que tentem monitorar seu tráfego. O navegador também garante que nenhuma transmissão Tor possa revelar, ao mesmo tempo, sua localização na Internet e os sites que você visita - embora alguns deles (sites ou terceiros) reconheçam um ou outro.

COMO USAR?

O Navegador Tor está disponível para GNU Linux, Mac OS, Microsoft Windows e sistemas operacionais do Android. Para usar em seu computador, é necessário apenas instalá-lo através da página do Projeto Tor (link abaixo). Já para usar no celular, é necessário a combinação de dois aplicativos: Orbot (para habilitar a rede Tor) e Orfox (para iniciar o navegador anônimo e seguro).

REFERÊNCIAS

Navegador Tor para Windows
Projeto Tor
Orbot e Orfox

COMO FUNCIONA?

Tecnicamente, para acessar uma página online, você precisa que seu provedor de Internet (ISP) conecte seu dispositivo ao servidor web da página. O provedor precisa saber, então, qual o IP (ou endereço) da página que você quer acessar para que ele possa fazer a conexão, ou seja, o provedor sabe que páginas você está acessando. Se você estiver em um país que censura a Internet, no entanto, o provedor consultará uma lista de sites proibidos e então decidirá se deve ou não fazer a conexão.

Além disso, as páginas também podem ver quem se conecta a elas, através dos IPs de nossos dispositivos. Assim, quando você acessa uma página você está, ao mesmo tempo, informando ao seu provedor de Internet o IP da página e informando à página o IP do seu dispositivo. Isso acontece, na verdade, com grande parte dos serviços online que acessamos, não só com páginas.

Para não cair na censura ou para ter sua privacidade resguardada enquanto navega na Internet, você pode usar uma VPN (*Virtual Privacy Network*).

A *Virtual Privacy Network* ou Rede Virtual Privada é um serviço que liga seu dispositivo a um outro dispositivo através de uma conexão criptografada. Assim, todo o seu tráfego de rede passa primeiro por esse dispositivo, e depois vai para a Internet. Isso significa que nem o seu provedor de Internet consegue ver que serviços você está acessando, nem os serviços conseguem ver o seu endereço de IP. A VPN mascara seu endereço de IP e faz parecer que você está em outro lugar, evitando assim a censura e a exposição. Além disso, ela criptografa toda sua conexão.

Mas ATENÇÃO: o dispositivo intermediário pode ver todo o seu tráfego, o que faz com que nem toda VPN seja confiável.

QUAL VPN USAR?

Nós recomendamos algumas VPNs:

> A VPN do coletivo Riseup
> A VPN do coletivo Autistici/Inventati
> A VPN do coletivo AktiviX - pra usar, tem que pedir por e-mail
> Essa não é ativista e é paga, mas é segura, Private Internet Access

EMAIL SEGURO

COMO FUNCIONA?

Se você já sabe *Como Funciona a Internet*, sabe também que nossas informações básicas de metadados circulam pela Internet e por seu provedor e servidor de e-mail. Um serviço de e-mail seguro é aquele que se compromete a não acessar seus e-mails, vendê-los ou ceder suas informações pessoais e de metadados a terceiros. Os e-mail tradicionais, sejam os de grandes multinacionais ou de pequenas empresas, não costumam oferecer esse tipo de proteção, além de alguns exigirem métodos de identificação pessoal (cópia de RG etc). Um servidor de e-mail seguro, além de garantir seu anonimato, também fornecerá conexão criptografada e, se possível, sua caixa de e-mails também criptografada. Esses serviços, em geral, são mantidos por grupos e pessoas que acreditam em uma internet livre e aberta, que atuam contra a censura e a favor de um outro mundo, mais acessível.

RECOMENDADOS

Alguns servidores - ativistas - fornecem e-mails seguros. Como as despesas para manter servidores de e-mails são altas, eles restringem o uso a grupos e pessoas ativistas ou de confiança. Conheça alguns:

> *Riseup.net - é necessário ter um convite para se registrar: peça a alguma pessoa que você conhece que tem conta lá;*

> *Autistici.org - uma pequena, porém sincera apresentação pode te garantir um e-mail seguro;*

> *Resist.ca - um formulário para saber mais sobre você e seus princípios pode garantir ou não uma conta neste servidor ativista*

KEEPASSX

O QUE É?

O KeePassX é uma ferramenta permite armazenar e gerenciar múltiplas senhas dentro de um arquivo de banco de dados criptografado. Esse arquivo é criptografado com uma senha-mestra que você mesma cria. O KeePassX também pode ser usado para gerar senhas fortes para suas contas através de parâmetros definidos por você.

Como o banco de dados gerado por ele é criptografado, você pode armazenar cópias em vários lugares, o que torna o backup de suas senhas relativamente simples. Nós não recomendamos enviar o seu banco de dados por e-mail ou armazená-lo online onde outras pessoas poderiam ter acesso. Muitos usuários do KeePassX mantém uma cópia no seu computador principal, uma cópia em um dispositivo USB e uma cópia em seu disco de backup.

COMO USAR

O KeePassX está disponível para GNU Linux, Windows e Mac OS X. Você pode baixar diretamente do site ou do seu gerenciador de pacotes, caso use GNU Linux ou Mac OS X. Ao iniciar o KeePassX você deverá criar um novo banco de dados (será um arquivo salvo no seu computador ou onde você preferir) que pode conter suas senhas pessoais, senhas do seu trabalho, ou qualquer outra coisa. Esse banco de dados pode ser definido através de categorias (e-mail, sites, compras, servidor etc) onde você pode registrar seu login, sua senha, alguma dica, entre outras coisas. Além disso, você pode copiar sua senha diretamente de seu banco de dados, sem necessariamente vê-la.

REFERÊNCIAS

> Como instalar KeePassX

> Como fazer e manter senhas seguras

REUNIÕES EM GRUPO ONLINE E SEGURAS

COMO FUNCIONA?

Para fazer reuniões ou conferências online com múltiplas pessoas através de áudio e chat seguros é possível usar os programas Jitsi ou Mumble, dois programas livres e de código aberto que possuem criptografia ponta a ponta, e que funcionam em Windows, Linux e OS. Há também os provedores do serviço Jitsi online (Jitsi Meet), que não requerem instalação de software.

O Jitsi é uma ferramenta para videoconferência que fornece criptografia de ponta a ponta para conversas de voz (ZRTP sobre SIP). Seu uso mais comum é por meio dos serviços online, hospedados pelo próprio Jisti ou pela Greenhost. Com eles, é possível criar salas seguras para as conversas sem ter que instalar nada, direto do navegador de internet. Basta criar um ambiente e passar o endereço de acesso para as outras pessoas, que também poderão acessá-lo de seus navegadores. Para quem depende do celular, o aplicativo Jitsi Meet busca simplificar este acesso.

Já o Mumble é uma ferramenta de audioconferência, sem suporte a vídeo, que pode ser usada para reuniões entre duas ou mais pessoas. É preciso instalar o programa ou o aplicativo de celular (Plumble para Android e Mumble para iOS) e usar o servidor padrão Murmur. Também é possível instalá-lo em um servidor próprio. O Mumble se conecta via TLS e o áudio é criptografado com AES. Além disso, permite autenticação por senha para as pessoas usuárias.

OUTRAS FUNCIONALIDADES

A versão instalável do Jitsi também pode ser usada como um programa de mensagens seguras (messenger). Como o Jitsi é compatível com o Facebook Messenger e com outros protocolos populares de telefonia (Jabber/XMPP, AIM, ICQ, MSN, Yahoo! Messenger e SIP), basta configurá-lo para usar suas contas já existentes. Neste caso, o ganho é poder proteger as conversas de texto usando o protocolo OTR (Off-the-Record), de criptografia ponta a ponta.

O conteúdo da sua comunicação passa a ficar inacessível a terceiros, tais como governo ou plataformas de vigilância corporativas, além do próprio serviço de troca de mensagens - se você estiver usando o Facebook Messenger, o Facebook; se você estiver usando Google Talk, o Google.

REDES MESH

COMO FUNCIONA?

‘Redes mesh’ são redes computacionais distribuídas. Nos últimos anos, tem se popularizado o conceito de redes autônomas (ou redes livres) como a infraestrutura alternativa de uma comunidade. Redes autônomas são construídas em um bairro, uma vila/aldeia ou uma cidade, normalmente pelos próprios moradores, em um processo colaborativo. São bastante populares em áreas carentes de infraestrutura e podem ou não prover acesso a internet. Suas principais características são:

> Estrutura distribuída. O crescimento é possível a partir de qualquer ponto;
> Respeita a neutralidade da rede;
> A comunidade deve ter autonomia para manter sua rede e seus serviços sem o apoio de empresas.

CONSIDERAÇÕES SOBRE SEGURANÇA

Usar serviços locais de rede como chat, telefonia e troca de arquivos evita que suas informações trafeguem pela rede de empresas e governos. Essa autonomia atrai comunidades preocupadas com privacidade a investir em infraestrutura própria administrada por pessoas de confiança. Apesar disso, o uso de criptografia forte e demais práticas de segurança holística devem ser mantidas, pois é sempre possível que pessoas infiltradas acessem essa rede e exponham informações vulneráveis das demais pessoas usuárias.

REFERÊNCIAS

Projeto Rizoma de Redes Livres - a possibilidade de criar uma infra-estrutura de comunicação popular que seja aberta, descentralizada e gerida pelos seus próprios usuários
Introdução a Redes Autônomas do Coletivo Vedetas
Wiki de documentação da Coolab

Por: Carla Jancz

MENSAGERIA SEGURA

COMO FUNCIONA?

Há muitos aplicativos de comunicação assíncrona, isto é, mensagens que podem ser recebidas mesmo se uma das partes estiver offline ou indisponível. Para listar alguns aplicativos desse tipo de comunicação: WhatsApp, Signal, Telegram, Threema, Viber, Wire. Embora alguns deles prometam segurança e privacidade das comunicações dos seus usuários, há algumas decisões e especificações que deverão ser levadas em conta ao optar por utilizá-los. A primeira delas é se o software do aplicativo e o código que é executado no servidor é aberto/livre ou fechado/proprietário. Isso significa que se for proprietário, não é trivial saber como funciona a sua segurança. A segunda é que não basta apenas saber se é criptografado, mas também conhecer qual é o tipo de criptografia utilizada e, ainda, se ela segue as boas práticas da área. A terceira questão é o que a empresa ou a organização responsável fez no passado ao ser solicitada para entregar os dados de seus usuários para as autoridades (de qualquer país). A quarta questão é conhecer o modelo de negócios do aplicativo: se ele não vende os dados do usuário, como ele paga a conta? Ele existirá no futuro ou é apenas mais uma startup?

COMO SE PROTEGER?

Não exponha informações sensíveis em aplicativos sem criptografia ponto a ponto em nenhuma situação. O Signal é desenvolvido pela WhisperSystems e possui a melhor avaliação quando realizamos as perguntas acima. É recomendado por especialistas da área da Segurança da Informação como, por exemplo, Edward Snowden, ex-analista de inteligência da NSA. Caso um contato use meios não criptografados para iniciar uma conversa, diga para a pessoa falar com você no Signal. Lembre-se de habilitar as mensagens efêmeras para que as mensagens sejam apagadas após um período e evite acumular muitos históricos de conversas. Sempre verifique pessoalmente a identidade dos seus contatos. É um processo rápido e que alertará qualquer mudança da identidade do seu contato.

REFERÊNCIAS

Campanha “Use Tor, Use Signal”

Por: Gustavo Gus

BACKUP

O QUE É?

Backup é uma cópia de segurança dos dados armazenados em seus dispositivos, como documentos, fotos, contatos, entre outros. Há várias maneiras de se fazer essa cópia de segurança: você pode configurar um programa para executar um backup rotineiramente, ou você pode fazer manualmente, copiando e transferindo seus dados de um dispositivo para outro. O objetivo é que você se resguarde de uma ocasional perda de arquivos originais, seja por ações despropositadas como perder um celular, pendrive ou ter um problema com seu HD, seja por apreensão dos equipamentos, ou ainda mal funcionamento dos sistemas. Ter uma cópia de segurança permite restaurar os dados perdidos.

COMO FAZER?

O backup pode ser feito em arquivos salvos no computador, no celular e no tablet, mas o ideal é armazenar cópias em dispositivos diferentes para garantir que não sejam perdidas. Não recomendamos usar nuvens (Dropbox, Google Drive) para backups, a não ser que você mantenha sua própria nuvem e, além disso, que seus dados estejam criptografados. Recomendamos, ainda, que o dispositivo do backup seja criptografado, para garantir que não será acessado por terceiros.

REFERÊNCIAS

Como se recuperar da perda de informações

SAFER NUDES - MANDA NUDES

COMO FUNCIONA?

Em tempos de “Pornô de vingança” (*Revenge Porn*), saber como enviar seus nudes é fundamental. O projeto Safer Nudes foi realizado pela organização Coding Rights para abordar o debate sobre privacidade online de uma maneira divertida. É um guia que defende o direito de fazer e mandar nudes como “uma prática de resistência prazerosa contra o machismo, o conservadorismo, o racismo e a heteronormatividade.” Assim, “publicá-los ou não deve ser uma escolha exclusivamente sua, no exercício do seu direito à privacidade."

DICAS

Safer Nudes é um guia sensual - em formato de zine, com instruções para se proteger ao enviar suas fotos. Algumas dicas são:

> Anonymize

> Use canais seguros na hora de compartilhar

> Use senhas fortes nas suas redes

> Não mostre seu rosto ou marcas/tatuagens que podem te identificar nas fotos!

Acesse o zine e pegue mais dicas!

REFERÊNCIAS

Safer Nudes

COMO FAZER UMA DENÚNCIA DE FORMA SEGURA

A IMPORTÂNCIA DE DENUNCIAR

Temos que lidar, dentro e fora de contextos ativistas e de movimentos sociais, com diferentes tipos de violência: assédio moral e sexual, abuso de poder, roubo, estupro, perseguição física e virtual, perseguição policial, intimidação, entre diversos outros. Essas violências têm a ver com as estruturas de poder estabelecidas nas relações entre as pessoas nesses diferentes contextos. Uma denúncia de um caso de violência pode ser uma ferramenta para reorganizar essas relações de poder. Entre os objetivos finais da denúncia estão o bem estar da pessoa denunciante, a responsabilização da pessoa denunciada e a ampliação da reflexão e consciência na comunidade envolvida, gerando potencial para mudanças.

RISCOS ENVOLVIDOS

O sucesso de uma denúncia depende de diversos fatores, como a efetividade das pessoas e instituições envolvidas no recebimento e encaminhamento da denúncia, o estado emocional e preparo prévio da pessoa denunciante, e o nível de influência e poder da pessoa denunciada. A elaboração de uma denúncia deve levar estes fatores em conta para ampliar a segurança física, mental e emocional da pessoa denunciante.

A violência que gera a necessidade de denúncia impacta na integridade física e mental da pessoa denunciante, que frequentemente já chega bastante fragilizada nos momentos de decisão e elaboração da denúncia. Um processo de denúncia feito sem a devida atenção pode piorar a situação de quem denuncia. Apoio físico e psicológico podem ser fundamental para garantir o bem estar da pessoa denunciante.

DENÚNCIAS ANÔNIMAS

Em certos casos, pode fazer sentido denunciar de forma anônima. Alguns órgãos e instituições inclusive têm políticas nesse sentido. Nesses casos, é importante contextualizar o que se entende por anonimidade para garantir que os efeitos pretendidos sejam atingidos e minimizar possíveis efeitos colaterais resultantes de falta de informação.

O ato de denunciar pode deixar rastros, seja ele feito pessoalmente, por telefone, carta ou internet. Se é importante que sua identidade seja ocultada, gaste um momento para pensar de que formas é possível reduzir os rastros. Alguns itens a levar em conta são a presença de câmeras de segurança, os registros de ligações telefônicas (não só dos números dos aparelhos mas também das torres de celular e horários das ligações), a possibilidade de gravação e de utilização de técnicas de reconhecimento facial e de voz, os registros de dados de navegação na Internet, etc.

Existe, também, um balanço entre credibilidade e anonimidade. A ocultação da informação de autoria costuma, ironicamente, ter efeitos opostos em denúncias reais e falsas. Por um lado, é importante que uma denúncia anônima real seja o mais precisa e completa possível para compensar a ocultação da autoria. Mas, por outro, também é importante evitar detalhes que possam acabar revelando a identidade da pessoa denunciante.

FORMAS DE DENUNCIAR

Existem diversos canais “oficiais” para denúncia online, tanto do Estado quanto de grandes empresas, ONGs e até grupos autônomos. Você pode fazer uma pesquisa para descobrir qual é o canal adequado de fazer uma denúncia. Para casos de publicações não autorizadas ou ameaças online, muitos sites fornecem meios de solicitar a remoção de conteúdos explícitos ou difamatórios.

É importante conhecer, também, formas alternativas de denunciar quando os meios oficiais não são suficientes. Manifestações artísticas e escrachos, por exemplo, são formas não institucionalizadas que foram encontradas por algumas pessoas para fazer sua denúncia mais efetiva.

Procure apoio de pessoas próximas e de confiança. Entrar em contato com grupos especializados também pode ser uma boa forma de se amparar durante o processo da denúncia. Contacte os grupos de confiança mais próximos a você, como grupos de mulheres, LGBT, coletivos técnicos que trabalhem com Segurança da Informação, etc.

Para denúncias anônimas na internet você pode utilizar o **Navegador Tor** ou o **Tails**. Leia sobre anonimidade online para evitar cair em erros comuns. Evite utilizar e-mails comerciais ou redes sociais, pois são mais suscetíveis a monitoramento.

Talvez seu processo de denúncia implique a necessidade de uma ação judicial. Para informações sobre defensoria pública, disque **129**.

Para denúncias de violência contra a mulher, disque **180**.

Para denúncias contra violência, abuso sexual, agressões físicas e/ou psicológicas cometidas contra crianças e adolescentes, denúncias de pessoas em situação de rua, da população LGBT, de pessoas com deficiência e idosos, disque **100**.

REDES SOCIAIS MAIS SEGURAS

COMO FUNCIONA?

As plataformas de socialização na Internet nos permitem articular, gerenciar e movimentar nossos grupos de maneira mais prática, porém, incluem também vários problemas relacionados à segurança e à privacidade. Além de construírem uma grande mineração das nossas redes mais próximas e dos nossos contatos, tais plataformas podem muitas vezes vender nossos dados para grandes empresas. Nossa comunicação, quando num estado de exceção, pode ser interceptada legalmente.

No mínimo, o que podemos fazer é focar nossa proteção por meio da conscientização da estrutura de privacidade que essas redes nos permitem.

Configure sua linha do tempo de maneira que só pessoas amigas possam ver seus posts pessoais, e de maneira que ninguém possa postar nela além de você. Configure as opções de marcação em posts e fotos de maneira que você possa analisar e escolher antes que marcações podem vir à público. Isso evita que conteúdos sensíveis (como rede de amizades, localização, informações sobre a família) fiquem disponíveis para qualquer pessoa. Além disso, verifique sempre nas suas redes sociais:

> Quem pode ver minhas publicações?
> Quem pode ver meu perfil?
> Quem pode entrar em contato comigo?
> Quais aplicativos estão autorizados e/ou vinculados à minha rede social?

Veja também o tópico Mensageria Segura

Como se proteger e manter seus dados seguros ao usar serviços de rede social

REFERÊNCIAS

Configurações de Segurança para Redes Sociais

Suruba de dados: o troca-troca sem consentimento dos apps de encontros

[referências]

Esta guia não seria possível sem o uso de vários materiais que estão disponíveis na Internet, realizados por grupos comprometidos com a Internet livre e a antivigilância. Reunimos uma série de links que foram consultados e, algumas vezes, modificados para este material. Neles você poderá encontrar mais informações,e aprofundar seus conhecimentos. Aproveite!

Laísa Mendes | @Porto Alegre

REFERÊNCIAS E OUTROS LINKS RECOMENDADOS

Guia prático de combate a vigilância na internet: http://www.temboinalinha.org/

Guia prática de estratégia e táticas para a segurança digital feminista: http://feminismo.org.br/guia/guia-pratica-seguranca-cfemea.pdf

Guia para mandar nudes de maneira segura: https://www.codingrights.org/safernudes/

Guia de Autodefesa Digital: https://autodefesa.fluxo.info/

Ferramentas de Segurança Digital para Todas as Pessoas: https://securityinabox.org/pt/

Guia de Segurança para ir a protestos: http://protestos.org/

Eu e minha sombra - Assuma o controle de seus rastros: https://myshadow.org/pt

Vídeos - Introdução sobre privacidade: https://vrr.im/9d

Jogo para encontrar Infiltrados, da Pública: http://apublica.org/vigilancia/infiltrados/

Vedetas - Servidora Feminista para Grupos Feministas: https://vedetas.org/

Manual de Segurança para Defensores de Direitos Humanos em Risco: https://www.frontlinedefenders.org/pt/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk

Encurtador de links feminista e seguro: https://vrr.im/

CryptoRave - 24h de atividades, oficinas e festa em torno da criptografia: https://cryptorave.org/

Lavits - Rede Latinoamericana de Estudos sobre Vigilância, Tecnologia e Sociedade: http://lavits.org/?lang=pt

Princípios para uma Internet Feminista - https://www.genderit.org/sites/default/upload/fpi_v3.pdf

Cl4ndestina - Servidora Feminista: https://clandestina.io

Oficina Antivigilância: https://antivigilancia.org/pt/boletim-11-pt/

Escola de Ativismo: https://ativismo.org.br

Agradecemos a Graciela Saleiman,
forte apoiadora do campo da defesa de direitos.