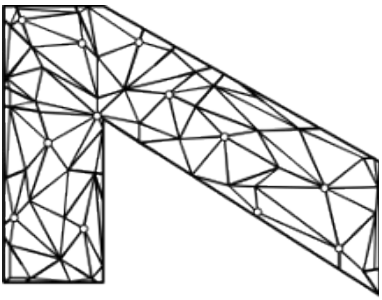
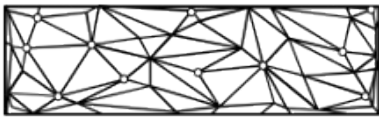
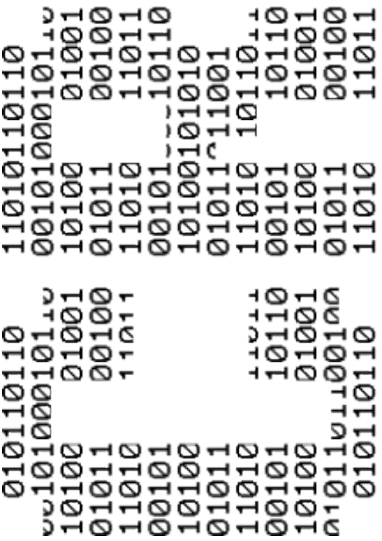




Cultura de Segurança e Comunicação Digital



segurança, criptografia, hacking,
anonimato, privacidade e liberdade na rede

CryptoRave

Inspirada no movimento das CryptoParties – eventos para pessoas comuns aprenderem a usar criptografia forte -, a CryptoRave surgiu no Brasil como um esforço coletivo para difundir os conceitos, a cultura e as ferramentas relacionadas à privacidade, segurança e liberdade na Internet. Chegando a sua quarta edição em 2017, a CryptoRave se consolidou como o maior evento aberto e gratuito deste tipo no mundo, justamente para ampliar o público que discute estes temas.

O evento conta com palestras, debates e oficinas para aprofundar e qualificar o debate sobre a proteção da privacidade na Internet como um direito e fundamento essencial à democracia. Ao final de 24 horas de atividades, uma grande festa: a Rave.

O evento é organizado por Actantes, Encripta Tudo, Escola de Ativismo, Intervozes, Saravá, ativistas e hackers independentes. Em comum, a defesa do direito à privacidade e do desenvolvimento de tecnologias de autodefesa em meio ao cenário de coleta massiva de dados.

Autodefesa

No espírito de compartilhar conhecimento e disseminar informações sobre privacidade, segurança e auto-defesa diante da vigilância massiva de Estados e empresas, a CryptoRave fez o esforço de, a partir do Guia de Autodefesa Digital produzir um mini-Guia introdutório de sobrevivência e autodefesa.

O caminho da autodefesa é proposto por consideramos que as pessoas devem ser responsáveis por sua própria segurança, não acreditamos em soluções prontas e sim na construção de uma cultura coletiva de segurança.

Para saber mais sobre como se defender, acesse o Guia completo em: https://autodefesa.fluxo.info/

Leia, use, passe pra frente o conhecimento!

Sem privacidade não há democracia

CryptoRave 2017 | https://cryptorave.org

"Na internet, ninguém sabe que você é um cachorro."

cartum de Peter Steiner, 1993

Autodefesa digital

Capacidade de uma pessoa ou grupo se proteger por conta própria de ameaças na comunicação eletrônica.

Por quê? A vigilância hoje é feita automaticamente e em larga escala: as pessoas são monitoradas mesmo que não sejam alvos específicos.

A seguir um roteiro inicial ajudar você a se proteger e tomar escolhas conscientes! Este também é um convite para que você se aprofunde mais no assunto.

Os Princípios Básicos:

1. **Segurança:** toda prática que nos ajuda a agir ao reconhecer e reduzir riscos.
2. **Paranoia:** é deixar de agir por conta de qualquer risco, real ou imaginário.
3. **Privacidade:** conjunto de informações que queremos proteger.
4. **Conforto:** quanto mais confortável e fácil for uma prática de segurança, mais chance ela tem de ser adotada. Cuidado com práticas super complicadas!
5. **Redução de danos:** adote procedimentos de segurança aos poucos, reduzindo os danos de forma sustentável, ao invés de tentar mudanças radicais que não sejam duradouras. Devagar e sempre!
6. **Economia:** procure adotar as práticas de segurança que sejam mais eficazes e menos custosas aos riscos que sejam mais prováveis! Uma boa segurança eleva o custo de alguém te atacar sem que você tenha um custo tão alto para se defender.
7. **Simplicidade:** não complique suas práticas desnecessariamente. A complexidade desnecessária pode criar falhas na segurança!
8. **Níveis:** uma boa segurança está presente em todos os níveis das tecnologias de comunicação, desde a segurança física dos dispositivos, passando pelos sistemas operacionais, pelos aplicativos e pelos protocolos de comunicação. O comprometimento de um dos níveis compromete no mínimo a segurança de todos os níveis superiores.
9. **Compartimentalização:** é a prática de segurança de isolar informações de acordo com a sua importância e necessidade. Por exemplo, falar com uma pessoa apenas o necessário para uma dada ação e manter algumas informações em círculos restritos de acesso.
10. **Obscuridade:** assuma que o inimigo conhece todas as suas defesas, mesmo que você não saiba se isso é verdade ou não. Isso vai te

ajudar a contar apenas com a eficácia das suas defesas, e não com o fato dela ser ou não ser conhecida.

11. **Abertura:** busque sempre usar hardware, software e protocolos livres e abertos, porque eles podem ser analisados publicamente, o que facilita a correção de falhas de segurança. Mas cuidado, não assuma que todo o software e hardware livre é seguro e livre de falhas. Liberdade e abertura tecnológica são condições necessárias para a segurança, mas não são condições suficientes para a segurança.
12. **Resiliência:** é a capacidade de resistir e se recuperar de ataques. Se as falhas não forem em pontos críticos, é possível se recuperar. Assim, é importante reduzir os pontos críticos de falha.
13. **Autoconsciência:** cultive seu senso crítico e não deixe que as práticas de segurança tirem a sua naturalidade de agir ao tornar você uma pessoa robotizada.

Segurança da Informação:

A segurança da informação é dividida em algumas propriedades:

1. **Confidencialidade:** é a garantia de que comunicação apenas poderá ser interpretada pelas partes envolvidas, isto é, mesmo havendo interceptação por terceiros, o conteúdo da comunicação estará protegido. Isso significa que, numa comunicação entre você e outra pessoa, haverá confidencialidade se apenas vocês tiverem acesso ao conteúdo da comunicação.
2. **Integridade:** é a garantia de que o conteúdo da comunicação não foi adulterado por terceiros. Ou seja, na comunicação entre você e outra pessoa, vocês conseguem identificar se alguém alterou o conteúdo das mensagens.
3. **Disponibilidade:** é a garantia de que o sistema de comunicação estará acessível sempre que necessário. Este é um requisito de segurança porque a falta de comunicação pode ser muito prejudicial.
4. **Autenticidade:** garante que cada uma das partes possa verificar se está de fato se comunicando com quem pensa estar se comunicando, isto é, a garantia de que não há um impostor do outro lado da comunicação.
5. **Não-repúdio**: garante que as partes envolvidas na comunicação não possam negar ter participado da comunicação. Esta propriedade é desejada em sistemas nos quais haja um controle sobre quem realizou determinados tipos de operações.
6. **Negação plausível:** o oposto do não-repúdio é a negação plausível,

no caso onde não é possível determinar com certeza se determinada pessoa participou da comunicação.

7. **Anonimato:** é garantia de que as partes envolvidas na comunicação não possam ser identificadas.

Nem sempre os sistemas satisfazem todas essas propriedades, seja intencionalmente ou não. É importante observar o que cada sistema oferece em termos dessas propriedades e se elas estão bem implementadas no sistema.

Por exemplo, alguns sistemas foram criados para possuir a propriedade do não-repúdio, enquanto outros são baseados na negação plausível.

Em muitas situações, é possível combinar diversos sistemas que ofereçam propriedades distintas de segurança da informação para obter o máximo de propriedades possíveis.

Limites da segurança

Viver é perigoso! Mas o que seria viver sem arriscar?

Segurança tem limites e faz parte de uma atitude segura saber quais são eles. Os principais são:

1. **Incompletude:** não existe segurança total ou sistema infalível. Todo sistema possui falhas.

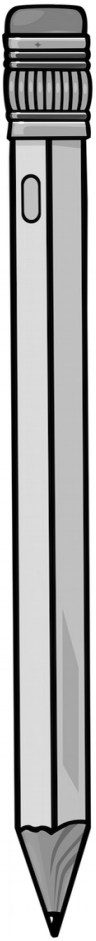
2. **Ceticismo:** é possível descobrir se sua segurança está sendo comprometida, mas isso nem sempre acontece. Pode ser que sua segurança esteja sendo comprometida sem que você saiba. Adote um ceticismo saudável para não ter ilusões sobre a sua segurança.

3. **Malícia:** nem sempre uma falha é resultado de um ataque intencional. Às vezes a comunicação tem problemas por falta de qualidade e não porque alguém esteja te atacando. Muitas vezes é difícil saber se você está sendo atacada/o ou se está sofrendo apenas uma falha de funcionamento num dispositivo.É sempre bom estar alerta e não baixar a guarda, mas você não precisa assumir logo de cara que está sendo atacada/o sempre que houver falha. Menos paranoia, mais senso crítico e intuição!

4. **Preparação:** prepare-se para a possibilidade da suas prática seguras falharem. Quando a casa cair, o que você vai fazer? Se preparar para isso também é uma prática segura!

Checklist

Mais do que sair adotando práticas e ferramentas de segurança, é importante que você tenha uma noção do todo e também das partes, ou seja, que você organize suas práticas de segurança num todo consistente.



Uma maneira fácil de fazer isso é manter um Checklist de Segurança:

1. Faça uma lista das suas atividades. Como cada uma delas funciona? Elas dependem de algum dispositivo tecnológico? Como eles funcionam em linhas gerais? Pesquise!
2. Quais são as ameaças envolvidas nessas suas atividades? Quem poderia te atacar? Como os dispositivos tecnológicos poderiam falhar? Pesquise e use a sua imaginação!
3. A partir do conhecimento reunido, como você poderia se proteger?

Existem diversos guias práticos sobre como se defender.
Por fim, **faça escolhas**:

- Comece pequeno e vá aos poucos. Você é capaz!
- Priorize as ameaças mais prováveis e as defesas que estejam ao alcance da sua capacidade. Cada pessoa tem seu ritmo.
- Segurança não é um fetiche: não adote uma prática só porque ela está na moda ou é considerada chique, mas sim se ela é útil para você.

Comunicação Digital

Nosso foco aqui é comunicação digital! Então vamos começar com nosso desenho esquemático da Teoria da Comunicação Hacker:

```
.                  grampo ativo ou passivo
                             |
                             |
Emissor/a ---meio----------meio-------------meio------ Emissor/a
Receptor/a         -----mensagem-1------>               Receptor/a
    1              <----mensagem-2-------                  2
```

Nesse desenho, duas partes envolvidas numa comunicação trocam mensagens entre si através de um meio que assumimos estar grampeado por padrão!

Ele não precisa estar necessariamente grampeado, mas se assumirmos que ele está, nós já estaremos nos preparando para as situações em que ele esteja!

Os ataques fundamentais da vigilância das comunicações são:

1. Interceptação de Dados: é a escuta do conteúdo da comunicação. Pode ser passiva – apenas grava a comunicação – ou ativa – quando também interfere na comunicação, alterando mensagens.

2. Interceptação de Metadados: quando apenas as informações básicas da comunicação são gravadas. Quem fala com quem, quando, onde, por quanto tempo, etc, sem que o conteúdo das mensagens seja obtido necessariamente.

É importante saber que algumas práticas de segurança protegem apenas os dados, enquanto outras protegem apenas os metadados da comunicação. Também existem práticas que protegem ambos!

Lembre-se que a vigilância é feita não apenas pelos governos, mas também por empresas.

Criptografia

Usamos criptografia para nos defender dos ataques à comunicação digital.

Ela codifica dados e/ou metadados para que a informação possua um ou mais critérios de segurança como confidencialidade, integridade e autenticididade.

Em sua aplicação mais básica, a criptografia é a técnica de codificar mensagens de tal modo que apenas quem possuir o segredo de como decodificá-las pode acessar seu conteúdo original.

Essas e outras propriedades da segurança da informação podem ser obtidas juntas ou separadas dependendo do sistema criptográfico em uso.

Hoje é essencial que meios de comunicação possuam algum tipo de criptografia, sendo essa uma condição básica para que resistam a ataques informacionais.

Para ser eficaz, a criptografia precisa usar padrões bem estabelecidos e ser bem implementada, do contrário ela só traz ilusão de segurança. Também é importante que a criptografia seja de ponta-a-ponta, isto é, que seja realizada integralmente nos dispositivos de comunicação das pessoas e não em dispositivos intermediários e que estejam fora do nosso controle.

Senhas

Para usar sistemas de comunicação com mais segurança é importante saber o básico e essencial sobre senhas.

Para ter acesso a determinados sistemas ou lugares, pode ser necessário fornecer uma prova de acesso para que ocorra uma **autenticação**, isto é, uma permissão de acesso.

Existem vários tipos de autenticação:

1. A autenticação pode ser baseada em algo que você carrega: por exemplo um cartão de crédito, um crachá ou documento de identificação.
2. A autenticação pode ser baseada em algo que só você ou um grupo restrito de pessoas sabe. Chamamos essa informação de **senha**.
3. Ela também pode se basear em alguma característica física sua e nesta caso estamos falando de **biometria**.

Aqui trataremos apenas sobre senhas, que é a forma de autenticação mais utilizada na comunicação digital. Biometria pode ser forjada e algo que você carrega no bolso pode ser roubado. Mas extrair uma senha da sua mente já envolve mais trabalho. Daí o poder das senhas!

Boas senhas possuem as seguintes características:

1. **Memorizável:** uma senha muito difícil de lembrar pode levar ao seu esquecimento e ser difícil de digitar.
   Já uma senha muito fácil de lembrar também pode ser muito fácil de alguém descobrir. Senhas muito fáceis em geral também tem um tamanho pequeno, então pense num tamanho mínimo e memorizável quando criar sua senha.
2. **Difícil de descobrir:** quanto mais difícil de descobri-la, melhor. Mas isso pode acarretar numa complexidade da senha que a torna difícil de lembrar.
3. **Pouco ou não compartilhada:** se você usa a senha para uma coisa, e uma única coisa apenas, é mais difícil dela ser descoberta. Quanto mais compartilhada, maior o risco, pois a superfície de ataque à senha aumenta.
   Esta característica vem diretamente do princípio da compartimentalização: se uma senha for comprometida, o dano estaria restrito apenas a um ou poucos sistemas.
   Uma senha roubada pode ser usada como tentativa para invadir outros sistemas. Se você usa a mesma senha para mais de um sistema e ela for roubada, trate logo de mudar a senha em todos os sistemas.

Computadores

O computador se transformou no elemento básico da comunicação digital.

Existem muitas falhas nos computadores em todos os níveis: no hardware, no sistema operacional e nos programas utilizados, assim como muitas formas de se defender.

Medidas básicas de segurança para computadores incluem:

- Usar software livre, como o sistema operacional Debian GNU/Linux.
- Usar criptografia de armazenamento.
- Manter o sistema sempre atualizado.

  Consulte documentações específicas para mais detalhes :)

Telefones

Os smartphones são uma catástrofe em termos de segurança e privacidade:

1. Seu funcionamento é baseado no rastreamento do aparelho, ou seja, todo telefone móvel é um dispositivo de rastreamento.
2. Existem problemas no hardware dos telefones que permitem acesso especial pelas operadoras de telefonia ou atacantes especializados.
3. O smartphone é também um computador, possuindo diversas das vulnerabilidades existentes em computadores.
4. O smartphone foi feito intencionalmente para ser um coletor automáticos de informações. Essas informações seguem para diversas empresas que a utilizam de forma estratégica para levarem vantagem em relação a toda a sociedade. Muitas dessas informações também acabam nas mãos dos governos e outras organizações.

É muito difícil usar um telefone de forma segura pois a arquitetura dos smartphones joga o tempo todo contra a segurança e a privacidade. Aqui não há espaço para uma análise detalhada então deixamos apenas as dicas mais básicas:

1. Mantenha o sistema do seu telefone sempre atualizado.
2. Preste atenção nas permissões solicitadas por cada aplicativo que você instalar.

   Repare que aplicativos maliciosos podem encontrar maneiras de burlar restrições no sistema.
3. Quanto menos aplicativos você usar, melhor. Pense no que é essencial para você. Mesmo aplicativos que pareçam ser inofensivos podem causar danos.

4. Dê preferência para softwares livres ou abertos. Além da loja de aplicativos padrão do seu telefone, você pode instalar lojas que oferecem apenas softwares livres.
   Sempre procure uma opção livre e aberta antes de buscar por um software fechado.
5. Quando precisar ter uma conversa sigilosa com alguém, combine com a pessoa para que vocês deixem seus telefones em casa antes de se encontrarem. Isso evita rastreamento e gravação de conversas via smartphone.
   A medida mais simples e eficaz é não usar telefone, mas hoje em dia está cada vez mais difícil viver sem ele por conta de imposições sociais. Assim, pode ser necessário fazer um uso estratégico dessa tecnologia.

Segurança na Rede

Qualquer informação que enviamos na internet está sujeita à vigilância.

É fácil nos conscientizarmos de quais informações enviamos voluntariamente, porém é mais difícil perceber informações adicionais, ou metadados, que são enviados automaticamente pelos softwares e serviços que utilizamos.

Quais são as informações que nos identificam e rastreiam nossos hábitos?

Rastreadores embarcados nos sites, como coletores de estatísticas e botões do tipo "curtir" conseguem estimar se estamos autenticados na respectiva rede social, qual o nosso login, etc.

Uma única página da web pode vir embutida com rastreadores de diversos serviços.

Este é o grande resumo que vale para redes sociais, mensageria, dados de formulário, informações de buscas, etc: Basicamente **TUDO** o que você envia na internet pode ser guardado indefinidamente, integrado a bancos de dados ou vazado.

E bastam poucas dessas informações para que seja possível nos identificar unicamente.

Como podemos nos defender de uma situação em que qualquer interação pode ser registrada e utilizada indefinidamente? Existe uma saída para a segurança da informação ou este é o fim da privacidade?

Estas são boas perguntas. A história dirá. Por hora, temos algumas medidas de segurança possíveis para melhorar um pouco nossa situação.

1. Garantir a segurança da informação básica: a comunicação criptografada usando **HTTPS** é a forma básica de se transferir

informações na web.

O uso do HTTPS nos dá mais garantias de que estamos acessando o sítio legítimo e não uma versão falsa. Também garante que a comunicação não poderá ser interpretada ou adulterada por interceptadores.

O uso do HTTPS depende da oferta deste pelo site ou serviço que você queira acessar. Um sítio que use HTTPS terá o seu endereço no navegador começando por **https://**, como por exemplo **https://wikipedia.org**.

O fato do HTTPS estar disponível em um site não implica necessariamente que a conexão é segura. O HTTPS possui vários problemas, como a dependência da certificação criptográfica feita por terceiros que podem ser invadidos ou serem compelidos a emitir certificações falsas.

Ainda, o HTTPS pode estar mal implementado nos sites.

2. Usar logins e serviços somente quando necessário: você precisa estar autenticado(a) o tempo todo nas redes sociais? Quanto menos você usá-las, menos irão te rastrear.
3. Você pode utilizar um navegador especial feito para proteger a sua privacidade.

   Recomendamos que você utilize o **Tor Browser** no seu computador e, no seu smartphone, o **Orfox** juntamente com o **Orbot**.
   Ambos os softwares utilizam a rede **Tor**, que é uma plataforma de navegação mais anônima. Ela utiliza criptografia e uma grande rede de computadores distribuídos pela internet, que dificulta muito a localização dos usuários que estão navegando.
   O Tor Browser é um navegador que usa a rede **Tor** em todas as suas conexões. Isso significa que ao navegar usando o Tor Browser você já estará, por padrão, dificultando sua localização na internet.
   Mas **ATENÇÃO**: certifique-se de sempre usar conexão HTTPS ao acessar qualquer site usando o Tor Browser. Do contrário, você estará muito mais suscetível a ataques de interceptação e de site falso.
   O Tor Browser também possui uma série de modificações de segurança para que a sua navegação fique mais segura.
   Já o Orbot permite que seus aplicativos no smartphone utilizem a rede Tor.
4. Procure usar serviços que respeitem a sua privacidade e que não façam dinheiro a partir da coleta das suas informações.

Mensageria

A decisão de quais comunicadores instantâneos utilizar é muito importante. Aqui seguem dicas para que você tenha condições de escolher por conta própria:

1. **A aplicação de mensageria é bem estabelecida?** Existem inúmeros aplicativos para comunicação instantânea, muitos deles afirmando inclusive serem seguros quando não são. O primeiro fator de insegurança pode ser um aplicativo que em si é inseguro.

2. **No caso do aplicativo oferecer criptografia, ela é de ponto a ponto?** Ou o conteúdo das mensagens pode ser acessado pelo serviço de mensageria?
   Pode ser importante observar também se a criptografia de ponta a ponta oferece negação plausível e a possibilidade de identificar chaves a usuários.
   No geral, a criptografia do aplicativo é bem implementada?
   A criptografia opera também nos metadados?
   Nem sempre é fácil responder essas perguntas e por isso é importante ficar de olho nos aplicativos recomendados pela comunidade de segurança.

3. **Como é feito o login na aplicação?**
   Aplicativos que funcionam no computador, em geral, possuem autenticação com senha. Mas, no caso dos comunicadores de celular, a criação de contas envolve a checagem com número de telefone como identificador global de usuários.
   Isso tem vários problemas. O número de telefone não é um dado anônimo e nem propriedade do usuário, mas sim da companhia telefônica. Além disso, se mal implementada, essa confirmação pode ser burlada por atacantes para roubar sua conta ou espionarem a sua comunicação.

4. **Onde ficam armazenadas as mensagens?**
   É importante saber se as mensagens ainda não entregues ficam armazenadas no servidor sem criptografia. E, se depois de entregues, ficam armazenadas no dispositivo do usuário também sem criptografia.

Softwares Recomendados

No smartphone:

- Signal Messenger para comunicação instantânea.
- Orbot e Orfox para navegação anônima.
- No Android, use a central de aplicativos livres F-Droid.
- Se possível, utilize um sistema operacional livre como o LineageOS.

No computador:

- Adote um sistema operacional livre, como o Debian GNU/Linux.
- Use o Tor Browser Bundle para navegação na web com mais anonimato.
- Para situações críticas, use o Tails, um sistema operacional livre e mais seguro.

Referências

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

→ Tem boi na linha? Guia prático de combate à vigilância na internet - https://temboinalinha.org

→ A Criptografia Funciona - Como Proteger Sua Privacidade na Era da Vigilância em Massa - https://we.riseup.net/deriva/a-criptografia-funciona-como-proteger+260170

→ Security in a Box - Ferramentas de Segurança Digital para todas as pessoas - https://securityinabox.org/pt/

→ PRISM Break - https://prism-break.org/pt/

→ Guia de Protestos - https://protestos.org

metadados coletados quando usamos celular