


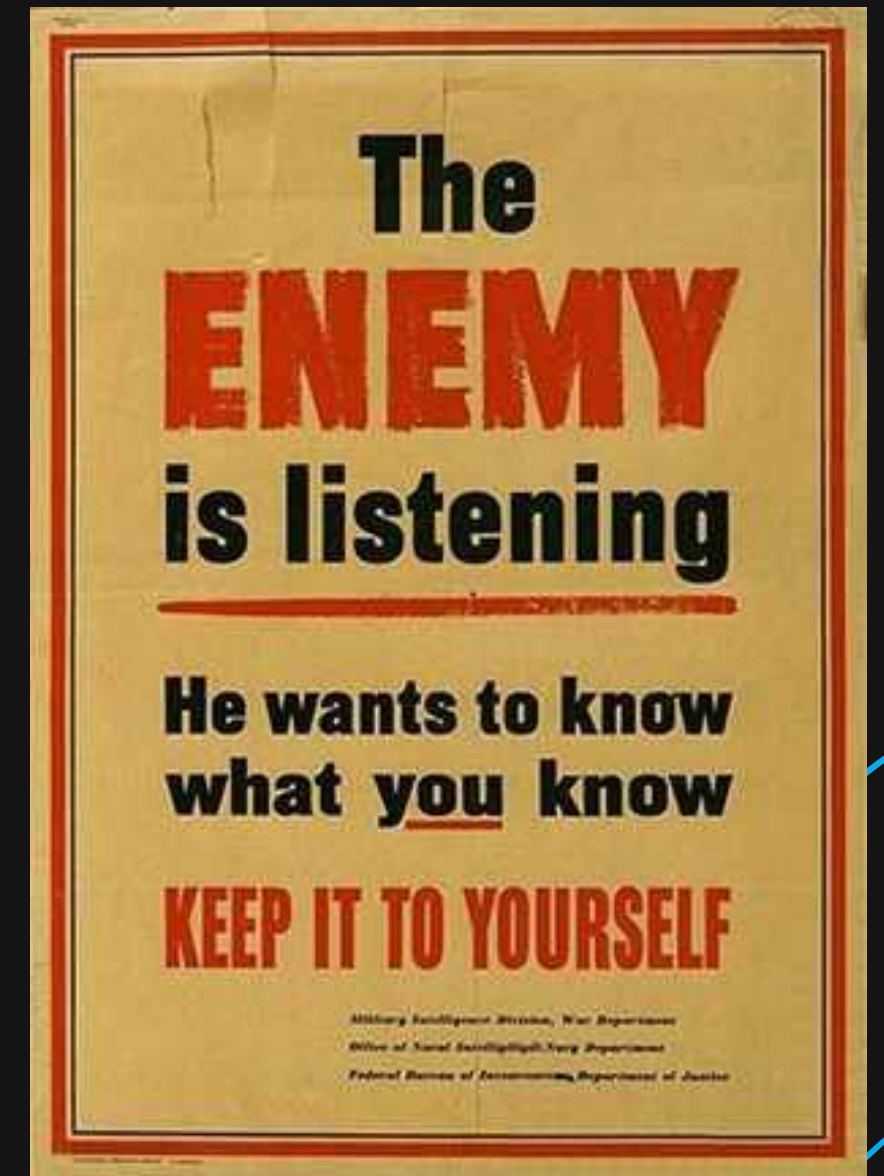
# Segurança da informação & Privacidade digital

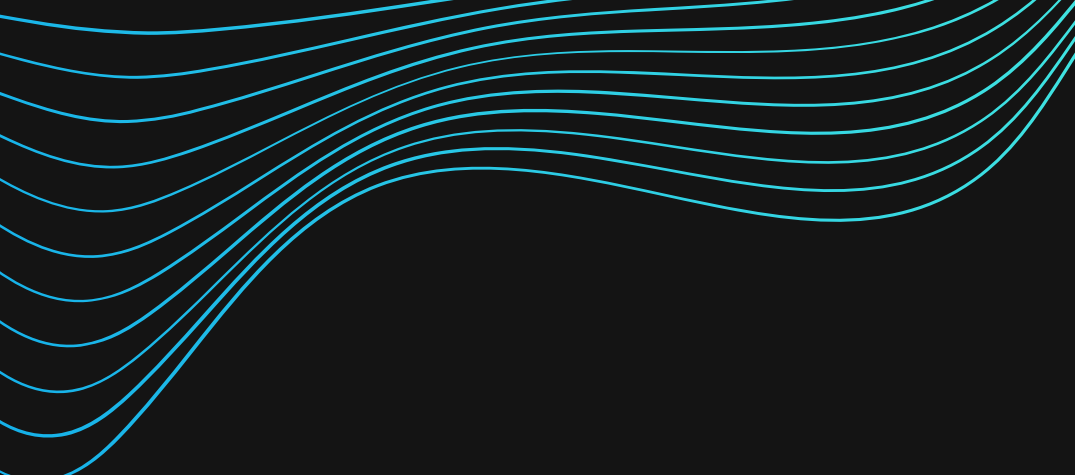
An abstract graphic consisting of numerous thin, light blue lines that flow and curve across the dark background, creating a sense of movement and digital connectivity.

Por Hermano J. B. Filho

# O inimigo está escutando...

Estamos o tempo todo trocando informações com inúmeras pessoas, mas com quais pessoas e que tipo de informações estamos passando? Você está sob um risco constante de ter suas informações sendo utilizadas contra você mesmo. Então se faz importante você ter consciência e controle do que você fala ou demonstra, a este cuidado damos o nome de OPSEC, ou segurança operacional. Lembre-se, o inimigo está escutando...





# Quem, o quê, quando, por que?

Primeiro de tudo, quem? Quem está me escutando e por que eu deveria me preocupar? É algo que você deveria sempre se perguntar, pare e pense sobre esta pessoa, se você realmente a conhece, se pode oferecer algum risco, tente entender quem é o interlocutor, para assim medir as informações que você irá passar.

# A informação em si

Agora que você parou para analisar com quem você está falando, está na hora de escolher as palavras certas, digamos assim. Talvez toda essa reflexão que fizemos até aqui o faça pensar que você só deve confiar só em si mesmo, e meio que por aí, mas na vida real nós confiamos em pessoas, precisamos confiar, faz parte da convivência, mas pense no que você está dizendo e como isso pode ser utilizado, como você pode ser identificado e acabar sendo alvo de ataques dos mais variados tipos.

# Imagine a seguinte situação...

Você é uma pessoa que costuma jogar jogos online, conhece alguém por lá e acabam se aproximando, se tornam amigos e começam a jogar constantemente, sempre conversam e aparentemente esta pessoa é totalmente confiável e gente fina, esta pessoa um dia te pede sua conta do jogo para subir o nível ou algo do tipo, prontamente você fornece seu e-mail e senha, alguns minutos depois percebe que não apenas sua conta de jogo mas como sua conta de e-mail e outras contas atreladas simplesmente saíram de sua posse...

Parabéns, você caiu na armadilha da Engenharia Social, você foi induzido a crer em uma história para fornecer ao atacante o que ele queria.



# A Engenharia Social

De nada adianta todo um sistema complexo de segurança se o usuário não está pronto para lidar com a maior vulnerabilidade possível, o fator humano. Não faz sentido toda uma estrutura de muros e portões vigiados se o porteiro deixa qualquer um entrar, e nisso consiste a Engenharia Social, explorar as falhas que existem na pessoa propriamente dita, na sua ingenuidade, na sua fraqueza psicológica, não importa, o engenheiro social é treinado para caçar e explorar qualquer falha que exista dentro da sua cabeça, e então você fará o que ele quer que seja feito.

A modalidade de ataque mais famosa desse estilo é o phishing.

# O Phishing

O phishing consiste em ser uma fachada, algo que parece ser autêntico, porém sendo uma armadilha por debaixo dos panos, imagine que você está acessando a página de login da sua rede social (ou pense que está acessando), você coloca seus dados e envia, contudo, seus dados foram enviados para um outro destino, de alguém que quer capturar sua conta, e agora você está em apuros. A forma mais comum de se aplicar o phishing é por meio de e-mails supostamente legítimos, da sua empresa, da sua rede social, ou coisa do tipo, pensados para te enganar e induzir ao erro.



# Como se proteger?

## VERIFIQUE QUEM ESTÁ TE MANDANDO

É um e-mail legítimo? É o contato de um conhecido? Tente verificar no portal oficial ou com a pessoa responsável, tenha certeza a fiabilidade do processo. Quando o e-mail é legítimo, há mais informações sobre a empresa, como outras formas em que o usuário pode entrar em contato. Veja também se há assinatura.

## ANALISE A NATUREZA DO CONTEÚDO

É algo que costuma acontecer? As informações procedem? Existem controvérsias no contexto mostrado? Algum possível erro ortográfico?

## SE ATENTE AOS PONTOS CHAVE

E-mails oficiais costumam ter seu nome ou alguma informação real sua, mas até isso pode ser armado, então tenha certeza de quem está enviando. Empresas normalmente não solicitam informações sigilosas (como número de cartão), então preste atenção nestes detalhes



# Boas práticas de segurança

Sempre bom ter um conjunto de práticas que evitem riscos, é como dizem, conhecimento não pesa, e também não custa nada ;)



# Boas práticas



## NUNCA USE A MESMA SENHA

Assim você diminui um risco sistêmico, se uma conta sua cair, não levará as outras junto. Você não vai lembrar de todas as senhas, eu sei, você sabe, então seria útil utilizar um gerenciador de senhas, como o BitWarden.

## USE VERIFICAÇÃO DE DOIS FATORES

Para ter uma garantia de segurança, evita que alguém com sua senha consiga acessar suas contas.

## USE GUIA ANÔNIMA/PRIVADA FORA DE CASA

Evite que logs, cookies e senhas sejam salvas em navegadores de máquinas externas.

## VERIFIQUE AS PERMISSÕES DE SEUS APPS

Veja se o app que você baixou realmente condiz com as permissões solicitadas, evite coisas como um spyware. Ex: uma calculadora não precisa acessar sua câmera.



# Boas práticas



## CUBRA A CÂMERA DE SEU LAPTOP

Essa é clássica, sempre bom evitar ser vigiado pela sua própria câmera sendo manipulada por terceiros.

## TENHA BACKUP DAS COISAS IMPORTANTES

Em caso de perda de acesso, um backup pode ser a diferença entre vida e morte, em alguns casos literalmente.

## USE FERRAMENTAS CONFIÁVEIS

Só ter prestado atenção no último módulo :)

## USE VPN EM REDES ABERTAS

Será melhor explicado mais à frente

## EVITE ACESSAR DADOS SENSÍVEIS FORA DE CASA

Nunca se sabe o chão em que está pisando.

# Por que não foram recomendadas VPN's anteriormente?

Infelizmente é difícil recomendar uma VPN, pois é muita coisa em jogo, por lá irá passar todo o seu tráfego, e é necessário ter cautela nesses casos, existem muitas opções de VPN por aí, com seus inúmeros riscos, mas a preferência geral é a mesma, softwares de código aberto e comprometidos com a privacidade. Infelizmente em alguns casos nem esse comprometimento vale...

# Opções que utilizo



## **ProtonVPN (disponível na F-Droid)**

Dos mesmos desenvolvedores de ProtonMail, o ProtonVPN surge com a proposta de privacidade e zero logs que a Proton AG promete.



## **Calyx VPN (disponível na F-Droid)**

Criado pelo Calyx Institute, instituição sem fins lucrativos com a privacidade como fundamento essencial, é uma ferramenta gratuita e sem a necessidade de criar uma conta. Particularmente me agrada bastante.

**AVISO: NÃO SÃO RECOMENDAÇÕES,  
APENAS OPÇÕES QUE UTILIZO, NÃO  
LEVE COMO FERRAMENTAS PERFEITAS**



# Considerações finais

Sua privacidade é um direito fundamental, defenda-o, além de um direito, é um risco real, portando proteja-se, você não vai sair daqui blindado e à prova de ataques, mas é o primeiro passo.

# Fontes e links úteis

Canal CyberDef – YouTube

Canal PrivacyMap – YouTube

\*Sim, os canais são em português

[privacyguides.org](https://privacyguides.org)

[eff.org](https://eff.org)

[ssd.eff.org](https://ssd.eff.org)

[cartilha.cert.br](https://cartilha.cert.br)

# Segurança da Informação & Privacidade Digital



don't trust, verify

# Acabou...

Obrigado por acompanhar :)

