# Manual de Segurança Digital

CUT BRASIL
CENTRAL ÚNICA DOS TRABALHADORES

# Manual de Segurança Digital

CUT BRASIL
CENTRAL ÚNICA DOS TRABALHADORES

**Texto**
Rodolfo Avelino

**Edição**
Gonzaga do Monte e Solange do Espírito Santo

**Revisão**
Sonia Nabarrete

**Ilustrações**
Gilmar Machado

**Projeto Gráfico, Diagramação e Capa**
Emílio Font

**Impressão**
Realce Produções Gráficas Ltda

**Esta obra tem o apoio do Solidarity Center**

**CENTRAL ÚNICA DOS TRABALHADORES**
www.cut.org.br

2021

# Sumário

# Apresentação

A publicação do Manual de Segurança Digital encerra a série de publicações do projeto desenvolvido pela Secretaria de Políticas Sociais e Direitos Humanos da CUT em parceria com o Solidarity Center. Foi um processo virtuoso de debates e de publicações que agora se estende num programa de formação de dirigentes e militantes visando estabelecer uma cultura de segurança coletiva e individual no movimento sindical e nos movimentos populares.

Trata-se de uma iniciativa da maior importância, considerando o projeto autoritário do atual governo e das forças de direita e de extrema direita que o apoiam. Resistir a este projeto, forjando barreiras de defesa da democracia e avançando na luta política para derrotar a coligação de forças que apostam no retrocesso político e civilizatório, continua sendo nosso principal desafio.

Essa ação imprescindível não deve descuidar da política de segurança, com estratégia e ações orientadas a proteger nossas organizações, nossos dirigentes e nossos militantes. No confronto político, ficamos expostos e toda medida de proteção coletiva e individual é necessária.

O Manual que agora publicamos aborda o tema da segurança digital, contendo informações e orientações práticas que todos devemos observar quando nos movimentamos no universo da comunicação em redes sociais, quando utilizamos contas bancárias ou espaços públicos de acesso ao Wi-Fi.

Recomendamos o Manual como mais uma leitura imprescindível para militantes e dirigentes do movimento sindical e dos movimentos populares.

**Jandyra Uehara**
*Secretária de Políticas Sociais e Direitos Humanos da CUT*

**Sérgio Nobre**
*Presidente da CUT*

# Prefácio

Nossa comunicação é cada vez mais realizada por meio de computadores, celulares e redes digitais. Isso traz novos desafios para as pessoas. O principal deles é romper com a ideia de que as tecnologias de informação são neutras ou meros meios para obter o que queremos. Essa postura é incentivada pelas grandes empresas de tecnologia, que buscam apresentar seus produtos digitais como um passe de mágica e como algo que somente melhora nossa experiência. Temos que romper com a alienação técnica e começar a observar as implicações individuais e coletivas das tecnologias.

Um dos grandes problemas que enfrentamos no cenário digital é como proteger nossas informações e nossos dados. Segurança digital não se obtém somente usando um produto. Segurança é um processo. De que adianta colocarmos grades nas janelas se esquecemos de fechar a porta de casa? Precisamos mudar nossa postura. As tecnologias digitais são ambivalentes, podem nos beneficiar muito, mas, também, podem nos prejudicar.

Este Manual é uma iniciativa que visa dar informações básicas para a proteção do nosso cotidiano digital, para proteger informações importantes, sejam de crakers, de criminosos digitais ou das Big Techs e plataformas que buscam coletar nossos dados, romper nossa intimidade, saber tudo sobre cada uma e cada um de nós para poder interferir em nossas escolhas ou modular nosso comportamento.

Evitar que tomem nossa senha, que vasculhem nossos arquivos armazenados nos computadores, garantir que a comunicação não seja ouvida de modo indesejado e indevido, evitar vazamentos de dados sigilosos, enfim, aqui temos um pequeno e importante passo para construir um processo seguro das nossas vidas no cenário digital e dataficado.

Boa leitura,

**Sérgio Amadeu da Silveira**
*Professor da UFABC e pesquisador de redes digitais*

# 1. Introdução e cuidados iniciais[1]

Antes de falarmos sobre aplicativos seguros, antivírus, criptografia ou qualquer outro termo, devemos falar sobre os atores que causam as violações de segurança.

Nossa segurança, seja na vida cotidiana ou no mundo digital, é colocada em risco a partir do momento que alguma ameaça possa explorá-la.

Ameaças são agentes humanos, naturais, políticos e tecnológicos que, através de uma fragilidade – que também poderá ser humana, tecnológica ou natural –, causarão possíveis danos materiais, financeiros, à vida e à nossa reputação ou da nossa instituição.

Um dos primeiros passos para evoluirmos na cultura de segurança é identificarmos possíveis ameaças que podem causar algum tipo de risco pessoal ou institucional. Algumas perguntas podem ser lançadas para identificarmos potenciais ameaças:

*1. Este Manual foi escrito por **Rodolfo Avelino**, consultor da CUT e especialista em cibersegurança e proteção de dados. Realizou trabalhos de segurança digital em entidades como Fundação Perseu Abramo, MST, Partido dos Trabalhadores, Fundação Rosa Luxemburgo, Mídia Ninja, Fora do Eixo e Jornalistas Livres. É doutorando e pesquisador no Laboratório de Tecnologias Livres (LABLivre) da Universidade Federal do ABC.*

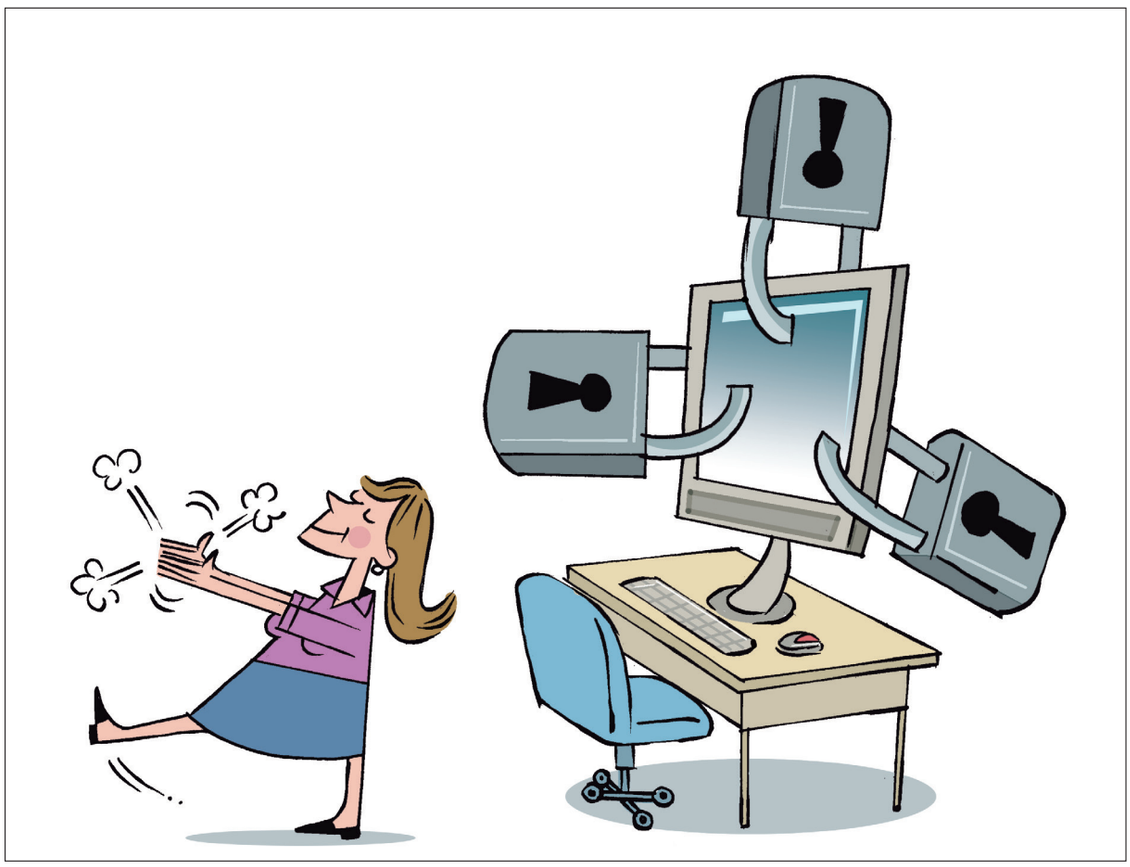
- Quem teria interesse nas mensagens armazenadas em meu equipamento?
- De quem eu quero proteger estes arquivos, fotos e vídeos?
- Existe algum risco se minha atual localização estiver acessível?
- Quem estaria interessado em interceptar minhas conversas?

As respostas poderão apontar para potenciais ameaças. Caso uma ameaça consiga infectar ou acessar seu dispositivo sem autorização, você pode enfrentar problemas como:

- Ter informações vazadas;
- Invasão de sua privacidade;
- Perdas financeiras;
- Ter seu equipamento danificado;
- Seu computador ou smartphone poderá ser usado para realizar ataques, aplicar golpes, infectar outros computadores, enviar mensagens em massa (spam) e disseminar vírus/malwares na Internet.

Por isso, precisamos desenvolver a cultura de segurança para que nossas informações, comunicação e dados estejam seguros no mundo digital.

# 2. Como construir senhas mais seguras



A senha ainda é um dos principais mecanismos de autenticação usados na Internet devido, sobretudo, à sua simplicidade. As principais violações de segurança e roubo de identidade são causadas geralmente por senhas comprometidas.

Depois de roubar as credenciais, os cibercriminosos podem usar as contas violadas para iniciar campanhas de desinformação, realizar fraudes e espionagem, entre outras atividades ilícitas.

Assim, para impedir alguém de ter acesso às nossas contas, a senha deve ser difícil de ser decifrada, e isso significa que ela deve ser forte o suficiente para evitar ataques de força bruta (quando insistem, por tentativa e erro, adivinhar sua senha).

Muitas pessoas não gostam de senhas, mas hoje elas são mais importantes do que nunca. Provavelmente uma senha que era segura há seis ou sete anos, é insegura hoje.

Geralmente as pessoas criam senhas fáceis de lembrar, o que significa que são curtas e simples, embora agora a maioria dos serviços tenha requisitos de comprimento mínimo e os tipos de caracteres que devem ser incluídos.

### Ao atualizar ou construir uma senha, evite cometer algum dos erros abaixo:

- Usar a mesma senha em vários serviços;
- Alterar a senha com um único caractere;
- Utilizar informações pessoais em senhas;
- Usar senhas pequenas;
- Criar senha usando uma sequência de teclas conhecidas. Exemplos: abc123, 123456, qwerty;
- Apenas substituir letras por números. Exemplos: c4s4, s1nd1c4t0, 4m4r3l0.

## 2.1 Sugestão para a criação de senhas diferentes para cada serviço

A seguir, apresentamos uma metodologia para a criação de senhas complexas e fortes que poderão ser utilizadas para a criação de senhas únicas para cada serviço.

A metodologia consiste em uma senha com no mínimo 3 (três) partes, sendo que cada uma delas será separada por um espaço.

**Parte 1** – Contém a porção com caracteres especiais e números.

**Parte 2** – Contém a porção da senha que você dificilmente irá esquecer. Aqui você pode usar uma senha que já utiliza há muito tempo, e com certeza não vai esquecer.

**Parte 3** – Nesta porção você pode indicar o nome do serviço ou sistema que você vai configurar a senha. Por exemplo, Facebook, Instagram, Gmail, entre outros.

No exemplo abaixo, as três partes estão configuradas assim:

Parte 1 = **4@ç**

Parte 2 = **Casaamarela**

Parte 3 = **email**

| Parte 1 | Parte 2 | Parte 3 |
|---|---|---|
| 4@ç | Casaamarela | email |

Observe que neste exemplo atendemos todos os requisitos na construção de senha dos principais serviços, ou seja, letras maiúsculas, caractere especial e número. Ao todo tem 21 caracteres contando os espaços.

O uso de "espaços" entre as partes cria uma dificuldade muito grande para o atacante e também para as ferramentas que tentam adivinhar sua senha, pois quase todas não possuem espaços em sua lista de tentativas.

## 2.2 Outras dicas para o gerenciamento e uso de senhas

ⓘ Alterar sua senha sempre que existir a suspeita ou indicação de comprometimento de sua confidencialidade;

ⓘ Modificar suas senhas regularmente, evitando reutilizá-las;

ⓘ Procure não salvar suas senhas quando um navegador sugerir esta operação. Se uma pessoa desconhecida acessar sua máquina ou até mesmo se ela for roubada, o criminoso terá acesso a todas as senhas salvas em seu computador;

## 2. Como construir senhas mais seguras

ⓘ Certifique-se que não tenha ninguém observando no momento em que você estiver digitando a sua senha;

ⓘ Usar senhas distintas para finalidades profissionais e pessoais;

ⓘ Coloque senhas mais complexas para serviços e sistemas que possuam informações sensíveis;

ⓘ Não compartilhe sua senha;

ⓘ Não escreva a senha em local público ou de fácil acesso (por exemplo, em pedaço de papel pregado no seu monitor);

ⓘ Não utilize números fáceis de serem descobertos, tais como os de telefone, data de nascimento, CEP de sua residência ou trabalho, CPF e números de outros documentos ou datas de qualquer espécie;

ⓘ Senhas fortes e únicas tornam muito mais difícil o acesso às suas contas pelos atacantes. Para protegê-las ainda mais, utilize autenticação de dois fatores quando possível;

ⓘ Se você puder escolher, prefira a aplicação de autenticação no celular (conforme exemplo no módulo de segurança em Redes Sociais) em vez de receber códigos por SMS. É mais fácil para um atacante redirecionar estes códigos para seu próprio telefone do que conseguir burlar o autenticador.

# 3. Cuidados na utilização de e-mails

ⓘ O e-mail ainda é o método mais utilizado para a disseminação de ataques;

ⓘ Nunca abra e-mails ou arquivos enviados por desconhecidos. Uma vez abertos, estes arquivos podem infectar seu equipamento;

ⓘ Não abra um anexo, a menos que esteja esperando por ele;

ⓘ Se possível, verifique os anexos com o antivírus antes de abri-los;

ⓘ Sempre que usar um computador emprestado, não esqueça de deslogar sua conta de e-mail;

ⓘ Não acredite ou confie em mensagens recebidas com assuntos como: atualização de dados cadastrais,

intimação da Policia Federal, fatura em atraso, sincronização de token, comprovante de transferência ou depósito, entre outras;

ⓘ Nunca acredite em mensagens com pedidos de correção de senhas, solicitação de quaisquer dados pessoais ou de documentos, pedidos de pagamentos;

ⓘ Evite ler e-mails em computadores públicos. Caso seja necessário, sempre opte por abri-los em uma "janela anônima" no navegador;

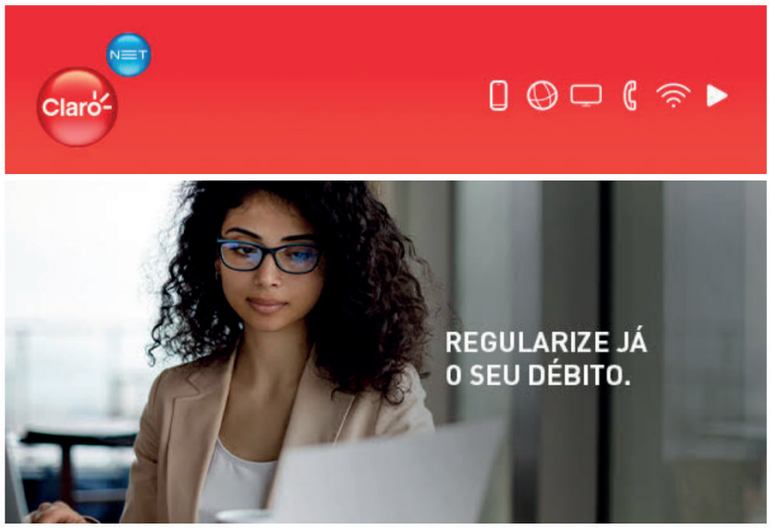
ⓘ Sempre esteja alerta ao conteúdo da mensagem e ao endereço de quem está enviando;

ⓘ Muitas vezes, falsos e-mails de bancos levam você a clicar em links que podem causar situações perigosas, como:

- ⓘ levá-lo a um site falso do seu banco para capturar o número da sua conta e senha;
- ⓘ instalar um programa malicioso em sua máquina para ter acesso a informações ou rastrear suas atividades;
- ⓘ Obter o controle de seu computador.

# 3. Cuidados na utilização de e-mails

Aqui é apresentado um exemplo de e-mail fraudulento que informa pagamento em atraso:




**Olá, RODOLFO**

Informamos que ainda não identificamos o pagamento da sua fatura vencida em 10/01/2021 no valor de R$ 487,58 Para sua comodidade, segue anexo PDF 2ª via da sua fatura Claro para pagamento.



Observe o nome de domínio do remetente (o nome que vem logo depois do @) desta mensagem:

from: **Fatura Digital - MINHA CLARO** <relacionamento@claroresidencial.com> via smtplw-03.com
to: RODOLFO
date: Feb 22, 2021, 5:15 PM
subject: Fatura em atraso RODOLFO
mailed-by: smtplw-03.com
security: Standard encryption (TLS) Learn more

O domínio é **@claroresidencial.com**. Geralmente, empresas brasileiras utilizam o domínio **.com.br**. Isso não quer dizer que devemos acreditar em todas as mensagens com o domínio **.com.br**, mas geralmente fraudes não possuem o **.br** no final.

Observe que esta mensagem traz um boleto em anexo, mas sem os dados do beneficiário.

Minha Claro residencial

2° VIA DE FATURA - CÓDIGO DE BARRAS

Nesse documento consta apenas o valor, vencimento e código de barras da sua fatura.

Este documento é válido para pagamento nos caixas de qualquer rede bancária ou com o código de barras abaixo no autoatendimento ou Internet Bank do seu banco. Utilize, preferencialmente, os bancos Santander, HSBC ou Bradesco.

Minha Claro residencial **RODOLFO**

Vencimento: **25/02/2021**
Valor: **R$ 487,58**

Autenticação mecânica

Pagamentos após o vencimento serão cobrados juros diários de 0,033% e multa de 2%.
Os encargos de pagamentos efetuados após o vencimento serão cobrados na próxima fatura.

Atenção efetue seus pagamentos nos bancos conveniados a seguir: BANCO BRADESCO S.A., BANCO COOPERATIVO DO BRASIL SA, BANCO COOPERATIVO SICREDI S/A, BANCO DE BRASILIA SA., BANCO DO BRASIL S.A., BANCO DO ESTADO DO PARA, BANCO ITAU S.A., BANCO MERCANTIL DO BRASIL S.A., BANCO REAL S.A., BANCO SAFRA S/A, BANCO SANTANDER, BANESPA/SANTANDER, BANRISUL, CAIXA ECONOMICA FEDERAL, CITIBANK, CPFL, HSBC BANK BRASIL S.A.

| CLIENTE | VENCIMENTO | VALOR |
|---|---|---|
| RODOLFO | 25/02/2021 | R$ 487,58 |

23793.38029 60974.111308 19006.333306 1 85420000048758

# 4. Cuidados na utilização de Internet Banking

Cada vez mais realizamos transações bancárias por meio do computador ou pelo aplicativo em nosso smartphone. As facilidades deste canal nos poupam de enfrentar filas ou até mesmo de ficarmos restritos aos horários de funcionamento das agências.

Entretanto, utilizar este canal de comunicação pode apresentar alguns riscos à segurança e requer cuidados. A seguir, recomendamos alguns procedimentos para que você possa realizar com mais segurança suas transações online:

# 4. Cuidados na utilização de Internet Banking

ⓘ Evite acessar sua conta bancária ou realizar compras online se estiver conectado em uma rede sem fio (Wi-Fi) pública (em restaurantes, bares, eventos, entre outros locais);

ⓘ Sempre acesse sua conta bancária em seu smartphone ou computador;

ⓘ Desconfie se o aplicativo ou site do banco solicitar mais de uma vez seu código de segurança;

ⓘ Evite inserir seus dados bancários ou de cartões em computadores compartilhados ou de terceiros;

ⓘ Sempre acesse sua conta usando a página ou o aplicativo fornecido pelo próprio banco;

ⓘ Digite o endereço do site bancário diretamente no navegador Web. Evite clicar em links recebidos e não utilize sites de busca para localizar seu banco;

ⓘ Sempre que concluir o uso do aplicativo, use a opção “sair”. Somente assim você garante que seu acesso foi finalizado.

# 5. Mantenha seus dispositivos atualizados

Muito provavelmente os seus dispositivos como notebooks e smartphones têm muito a contar sobre você. Caso uma pessoa mal intencionada tenha acesso ao seu celular por 30 minutos, ela saberá muito sobre você, como por exemplo, com quem você geralmente se relaciona, quais são suas preferências, quais foram suas últimas contas, suas últimas viagens e várias outras informações armazenadas em suas contas de e-mail, Redes Sociais, aplicativos de imagens e compras.

Para que este problema seja evitado, devemos manter nossos dispositivos atualizados e configurarmos algumas funções de segurança, como **usar preferencialmente programas com licença de uso livre (software livre) e programas originais**.

Sempre que precisar de um programa, pesquise e verifique se existe alguma alternativa livre e faça seu teste. Além disso, o uso de programas não originais pode colocar em risco a segurança do seu dispositivo, já que muitos deles não permitem realizar as atualizações de melhorias e segurança.

Também é possível que a instalação de programas não originais, obtidos de forma ilícita, inclua a instalação de códigos maliciosos. Seguem alguns alertas:

ⓘ Se você de fato tem preferência em usar programas proprietários, mas tem o costume de usar versões não originais, procure por alternativas gratuitas ou livres compatíveis e tente adaptar-se a elas. Essa é uma atitude política contra as práticas de monopólio de empresas transnacionais;

ⓘ Ao solicitar manutenção nos computadores de sua organização ou pessoal, não permita a instalação de programas não originais.

## 5.1 Atualize seus dispositivos com as últimas versões aplicadas

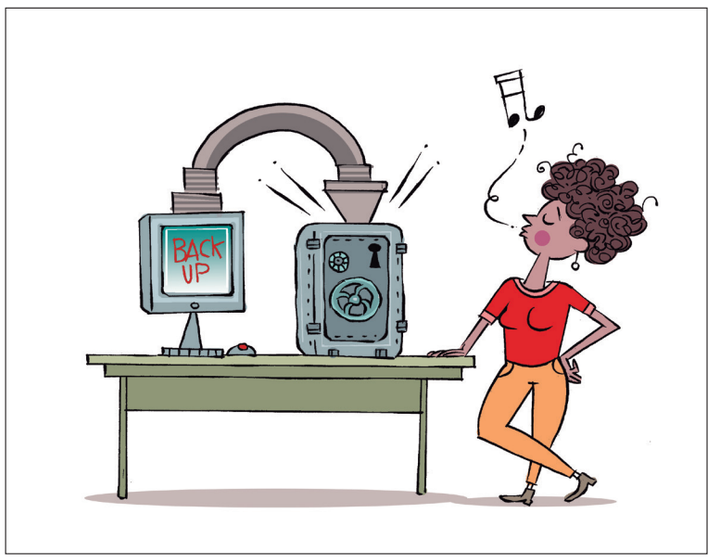
As atualizações evitam que vulnerabilidades conhecidas em seu sistema operacional e programas possam ser exploradas. Portanto, para manter os programas instalados livres de vulnerabilidades, além de manter as versões mais recentes, é importante que sejam aplicadas todas as atualizações disponíveis. Procure configurar seus dispositivos para que os programas sejam atualizados automaticamente.

## 5.2 Proteja seus dispositivos com senha e bloqueio por ociosidade

Sempre configure seus dispositivos com senha. Isso vai evitar que, por algum descuido, seu dispositivo seja acessado sem sua autorização. Configure seu dispositivo para que em um período curto de ociosidade ou sem interação, ele seja bloqueado. Além deste cuidado, lembre-se:

- Se for ao banheiro, bloqueie seu computador;
- Se for tomar café, bloqueie seu computador;
- Se for ali e já volta, bloqueie!

# 6. Faça backup dos seus dados regularmente




A informática nos trouxe algumas vantagens quando o assunto é a capacidade de armazenamento de documentos, fotos e músicas.

É muito possível que você possua em sua conta de e-mail ou no WhatsApp mensagens recebidas há mais de um ano e que contêm documentos estratégicos, financeiros e íntimos.

Caso seu equipamento seja furtado ou sua conta de e-mail ou WhatsApp invadidas, facilmente estas informações cairão em mãos erradas e poderão ser vazadas.

Além disso, quantas fotos e arquivos você já não perdeu quando seu equipamento teve que passar por uma manutenção ou até mesmo quando ele foi furtado?

Fica a dica: “Não devemos confiar plenamente na tecnologia”. Além dos problemas relacionados – de furto ou manutenção dos equipamentos –, manter arquivos estratégicos e sensíveis também pode comprometer a sua segurança e a da sua organização.

É extremamente recomendado que um e-mail recebido com algum tipo de informação que você acredita que não deve ser acessado por outras pessoas seja apagado assim que você o ler. Caso precise ainda daquela informação, salve o documento em seu computador pessoal (evite salvar em plataformas de armazenamento em nuvem como Google Drive e Dropbox) e apague-o logo em seguida de sua caixa de e-mail.

Para que as nossas informações estejam seguras contra furtos ou por necessidade de manutenções, devemos adotar a prática de fazer regularmente cópia de segurança destes documentos.

# 6. Faça backup dos seus dados regularmente

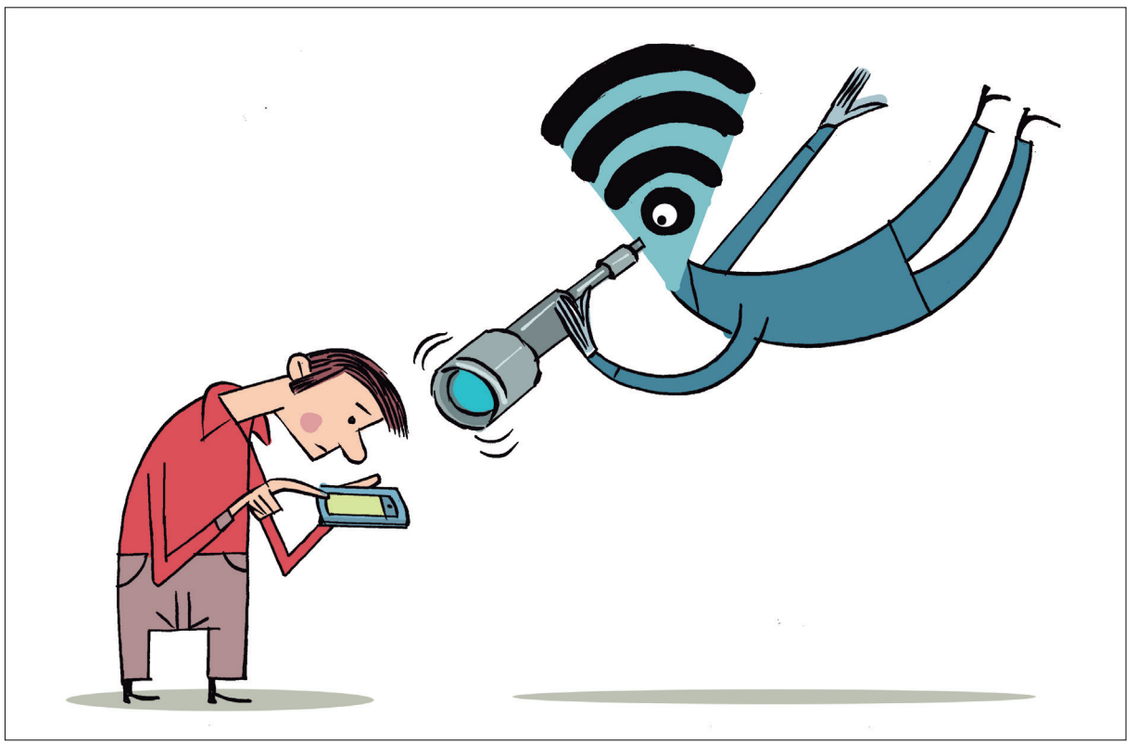
O termo técnico para cópia de segurança é backup. É recomendado que as fotos tiradas no celular, documentos burocráticos, contratos, entre outras informações sensíveis, sejam copiados para discos, HDs externos, outros computadores ou qualquer outro dispositivo.

## 6.1 Cuidados ao fazer suas cópias de segurança em mídias (pen drive e HD externo)

- É recomendado que os HDs externos sejam criptografados com softwares livres, como o Veracrypt (https://www.veracrypt.fr/en/Downloads.html);
- Tenha cuidado para não perder seus pen drives e HDs externos com as cópias;
- Sempre que possível, proteja suas mídias com senhas;
- Periodicamente, acesse suas mídias para confirmar se ela está funcionando e se seus dados estão íntegros;
- Ao descartar um pen drive, confirme se ele não possui dados armazenados;
- Mantenha as cópias gravadas em mídias em locais seguros, com acesso restrito e bem acondicionadas.

Realizar cópias de segurança também irá proteger você de ataques, como os conhecidos sequestradores de dados (**Ransomware**). Este tipo de ataque, ao infectar um computador ou servidor, criptografa todos os dados de sua organização. Então, procure saber se os dados de sua organização estão sendo copiados regularmente para outros locais.

# 7. Cuidados ao utilizar Wi-Fi público



Com planos de dados de telefonia móvel caros e restritivos, não há dúvidas que Internet Wi-Fi pública é conveniente, especialmente quando estamos trabalhando fora de casa ou escritório.

Além disso, algumas pessoas são viciadas em Wi-Fi livres e não hesitam em se conectar a uma rede disponível. Contudo, alguns cuidados devem ser tomados para que nossa privacidade e segurança não estejam em risco quando você utilizar uma conexão pública.

Muitas redes disponíveis em restaurantes, bares, eventos e espaços públicos têm suas senhas publicadas e de fácil acesso ou até mesmo não necessitam de autenticação. Esse cenário é uma ótima oportunidade para que criminosos possam realizar seus ataques para espionar, roubar informações e até mesmo redirecionar o seu tráfego para sites e servidores comprometidos.

Alguns cibercriminosos podem configurar um roteador wireless para se passar por uma rede legítima, embora sua in-

tenção seja apenas interceptar o tráfego de dados dos equipamentos que se conectarem a ele. Assim, os Wi-Fi públicos podem ser o paraíso de cibercriminosos.

Então, caso você tenha disponível um bom plano de dados, evite se conectar a uma rede pública. Mas se você tem mesmo a necessidade de fazer essa conexão, fique atento a estas dicas:

- Se a conexão for feita com seu notebook com Microsoft Windows, certifique-se de selecionar conexão "Pública" quando aparecer a opção, pois isso irá desativar possíveis pastas compartilhadas de seu sistema;
- Certifique-se que o firewall esteja habilitado;
- Tente visitar apenas sites com HTTPS habilitado. Fique atento se o endereço digitado é o mesmo apresentado na barra de endereço do site;
- Não use redes públicas para acessar informações sensíveis como Internet Banking, fornecer dados pessoais ou financeiros em formulário de sites, e realizar conversar confidenciais por meio dos aplicativos de mensagens;
- Quando se conectar a uma rede Wi-Fi pública, não escolha a opção "conectar automaticamente". Assim, toda vez que encontrar uma rede com o mesmo nome, o seu dispositivo sempre irá confirmar se você quer se conectar de fato. Nunca presuma que a rede que você usou em um lugar é tão segura quanto uma com o mesmo nome em outro lugar;
- Se você for usar uma rede Wi-Fi em restaurantes, rodoviárias ou aeroportos, onde é necessário criar um cadastro, evite colocar senhas que você já utiliza em outras ferramentas, como e-mails, bancos e Redes Sociais.

# 8. Códigos maliciosos

Alguns programas possuem a finalidade de executar atividades maliciosas e danosas em um dispositivo. Conhecidos como **Malwares**, estão entre as principais ferramentas de atacantes e cibercriminosos.

Caso o seu dispositivo seja infectado por um **Malware**, um atacante poderá ter acesso aos seus dados, mensagens armazenadas e também poderá executar ações fraudulentas e criminosas a partir de seu equipamento.

Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:

| Códigos Maliciosos | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Vírus | Worn | Bot | Trojan | Spyware | Backdoor | Rootkit |
| **Como é obtido:** | | | | | | | |
| Recebido automaticamente pela rede | | ✔ | ✔ | | | | |
| Recebido por e-mail | ✔ | ✔ | ✔ | ✔ | ✔ | | |
| Baixado de sites na internet | ✔ | ✔ | ✔ | ✔ | ✔ | | |
| Compartilhamento de arquivos | ✔ | ✔ | ✔ | ✔ | ✔ | | |
| Uso de mídias removíveis infectadas | ✔ | ✔ | ✔ | ✔ | ✔ | | |
| Redes sociais | ✔ | ✔ | ✔ | ✔ | ✔ | | |
| Mensagens instantâneas | ✔ | ✔ | ✔ | ✔ | ✔ | | |
| Inserido por um invasor | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Ação de outro código malicioso | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |

Fonte: Cartilha segurança CERT.br

Existem alguns **Malwares** usados para vigiar jornalistas investigativos, militantes e ativistas políticos. Eles são instalados em smartphones e têm a capacidade de interceptar ligações, mensagens, arquivos armazenados, e descobrir sua localização.

# 9. Segurança em smartphone

Os smartphones se tornaram o principal dispositivo para realizarmos nossas ações pessoais e profissionais. Cada vez mais este tipo de dispositivo vem se tornando o principal vetor de ataques de cibercriminosos, pois concentram informações atraentes e sensíveis, como um grande volume de dados pessoais armazenados. Além disso, são dispositivos fáceis de serem furtados.

# 9. Segurança em smartphone

A seguir, recomendamos alguns cuidados para proteger seus dispositivos e informações:

ⓘ Mantenha o sistema operacional e as aplicações instaladas sempre com a versão mais recente e com todas as atualizações aplicadas;

ⓘ Sempre apague conversas confidenciais de aplicativos de mensagens instantâneas, como WhatsApp, Signal e Telegram;

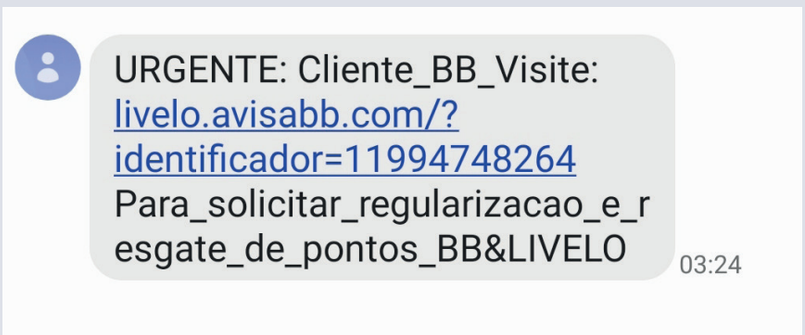
ⓘ Considere utilizar os mecanismos de segurança disponibilizados nos smartphones;

ⓘ Evite usar os recursos de biometria para o desbloqueio de funções (digitais e face);

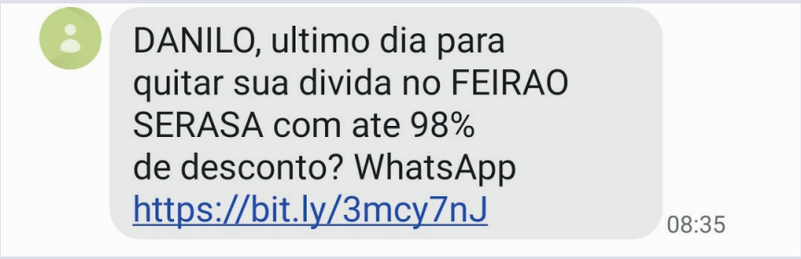
ⓘ Avalie a instalação de programas antimalware;

ⓘ Evite instalar programas desenvolvidos por terceiros, ou seja, que não estejam disponíveis no Google Play ou App Store;

ⓘ Seja cuidadoso ao clicar em links, a despeito de como foram recebidos e de quem os enviou. A imagem abaixo é um exemplo de mensagem maliciosa recebida por SMS:



ⓘ Seja cuidadoso ao clicar em links curtos e procure usar complementos que possibilitem visualizar o link de destino. A seguir um exemplo de um SMS com um link curto;




ⓘ Desabilite a autoexecução de vídeos e imagens em seus programas de mensagens como WhatsApp e Telegram;

ⓘ Faça regularmente backups de seu dispositivo e evite usar os recursos de backup das ferramentas como WhatsApp e Telegram;

ⓘ Mantenha interfaces de comunicação, como Bluetooth e Wi-Fi, desabilitadas e somente as habilite quando for necessário.

# 10. Cuidados na comunicação e Redes Sociais

A Internet foi uma das novidades mais revolucionárias do final do século XX. Não apenas pelo que ela realmente é, mas por tudo o que representa em nossas relações sociais, profissionais e no entretenimento.

A massificação de seu acesso vem impulsionando a quantidade e a circulação de dados pessoais nas redes digitais, alimentando maciçamente grandes bases de dados de nosso comportamento em servidores de grandes empresas, como Facebook, Google, Microsoft e Twitter.

Todas as pesquisas que realizamos no Google, as páginas que acessamos e os trajetos percorridos são exemplos de dados coletados mais comuns entre essas empresas. E, nesse sentido, sua onipresença em nosso cotidiano trouxe novos desafios para a privacidade.

A evolução dos dispositivos móveis e a difusão das possibili-

dades de acesso à Internet naturalmente qualificaram e permitiram o aprimoramento das ferramentas de rastreamento e vigilância, enriquecendo cada vez mais os mecanismos para personalização e identificação de usuários, sobretudo buscando entender sua experiência de navegação, seus relacionamentos e percursos, possibilitando assim lapidar as técnicas de controle e modulação de comportamento.

Sem dúvidas, as Redes Sociais permitem a nossa aproximação com amigos, familiares e parceiros. Além desta função básica, permitem a divulgação de eventos e o registro de momentos por meio de imagens, vídeos e áudio. Entretanto, se cuidados não forem tomados, ligações telefônicas, e-mails, mensagens instantâneas, fotos, vídeos e qualquer outro conteúdo que esteja em seu equipamento poderão ser acessados por pessoas mal intencionadas.

## 10.1 Alguns riscos relacionados às Redes Sociais

ⓘ Invasão de privacidade: muito cuidado com as informações divulgadas em suas Redes. Antes de publicá-las, avalie a real necessidade de compartilhá-las, pois elas poderão ser utilizadas em atividades maliciosas. Lembre-se que você está em um ambiente público e tudo que você compartilha poderá ser lido ou acessado por qualquer pessoa.

ⓘ Sequestro de perfil: é muito comum que cibercriminosos “sequestrem” seu perfil em Redes Sociais e ferramentas de mensagem instantânea para realizarem seus ataques ou simplesmente divulgarem informações falsas através de seu perfil.

ⓘ Perfil falso: você poderá ser alvo de ataques direcionados contra a sua reputação e, assim, o fraudador poderá ter acesso a suas imagens já publicadas e criar um perfil falso, tentando se passar por você.

# 11. Configurando e ajustando sua privacidade nas Redes Sociais

Quase todas as plataformas de Redes Sociais permitem ao usuário aplicar alguns controles predefinidos de privacidade. Não devemos ser inocentes e acreditar que essas configurações são suficientes para que nossa privacidade seja preservada. Alguns ajustes permitem que você bloqueie estranhos e pessoas que não são seus amigos de ver suas informações privadas.

Essas configurações também limitam as informações disponíveis nos resultados da pesquisa para que apenas seus amigos e grupos específicos ou até mesmo ninguém possa ver seu status, fotos, vídeos e interações nas Redes.

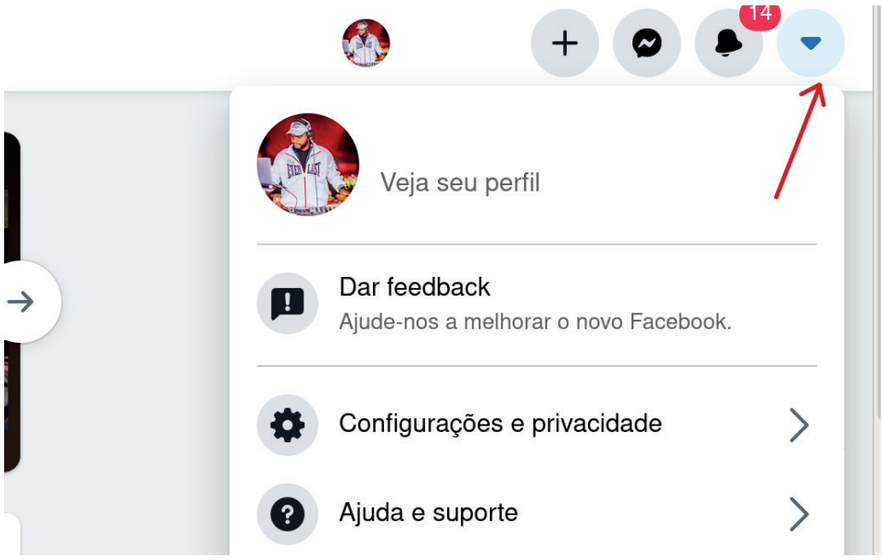
As configurações de privacidade podem ser ajustadas a qualquer momento. A seguir, vamos mostrar alguns exemplos de ajustes que poderão permitir seu controle e privacidade nas plataformas sociais.

# 11.1 Facebook

### Marcação em postagens

Desabilite a opção que permite outras pessoas marcarem você em alguma postagem. Acesse a sua página do Facebook no navegador de seu computador e siga os seguintes passos:

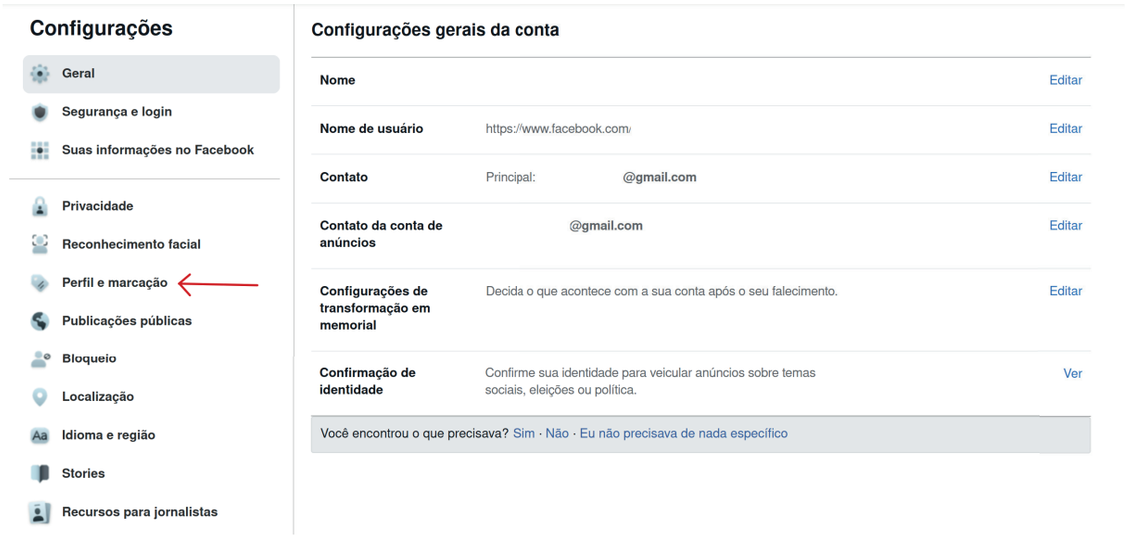
**1)** Depois de logado em sua conta, siga até o menu localizado no canto superior direito e clique no ícone. Quando aparecerem as opções, clique em **Configurações e privacidade**.




**2)** Clique na opção **Configurações**.

# 11. Configurando e ajustando sua privacidade nas Redes Sociais

**3)** No menu do lado direito clique em **Perfil e marcação**.




**4)** Na tela **Privacidade**, localize na opção **Marcações** o item **Quando você for marcado em uma publicação, quem você deseja adicionar ao público da publicação se essa pessoa ainda não puder vê-la?**. E escolha a opção **Somente eu**.


ⓘ Você sabia que suas atividades fora do Facebook, como transações online, bancos acessados, sites e outros aplicativos são enviados para ele?

# 11. Configurando e ajustando sua privacidade nas Redes Sociais

Não é surpresa para ninguém que suas atividades dentro do Facebook são monitoradas: curtidas, amigos mais acessados, sua localidade, lugares visitados, suas preferências, entre outras centenas de atividades.

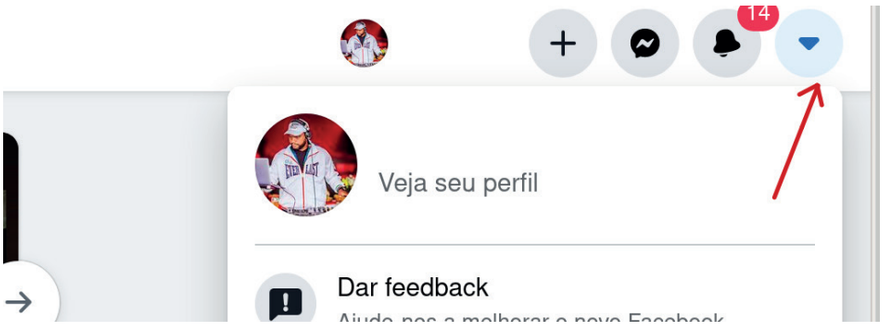
Agora é possível visualizar e desativar parte do monitoramento feito fora do Facebook. Batizada de **Atividade Fora do Facebook**, essa capacidade de visualizar e desativar estas atividades foi lançada em janeiro de 2020. Em sua página, o Facebook resume este tipo de monitoramento externo como:

*"A atividade fora do Facebook é um resumo da atividade que empresas e organizações compartilham conosco sobre as interações que você faz com elas, como visitas aos sites ou aos aplicativos. Elas usam nossas Ferramentas para Empresas, como o Login do Facebook ou o pixel do Facebook, para compartilhar essas informações."*

A figura abaixo explica como o Facebook usa parte das informações coletadas:

Siga os passos para desabilitar esta função:

**1)** Depois de logado em sua conta, vá até o menu localizado no canto superior direito e clique no ícone. Quando aparecerem as opções, clique em **Configurações e privacidade**.




**2)** No menu esquerdo da página de configurações, clique em **Suas informações no Facebook**.

# 11. Configurando e ajustando sua privacidade nas Redes Sociais

**3)** Ao abrir a página **Suas informações no Facebook**, clique em **Visualizar** no item **Atividade fora do Facebook**.


Ao clicar em **Visualizar**, a próxima tela apresentará um resumo sobre esta coleta de dados e alguns aplicativos que estão enviando as informações para o Facebook.

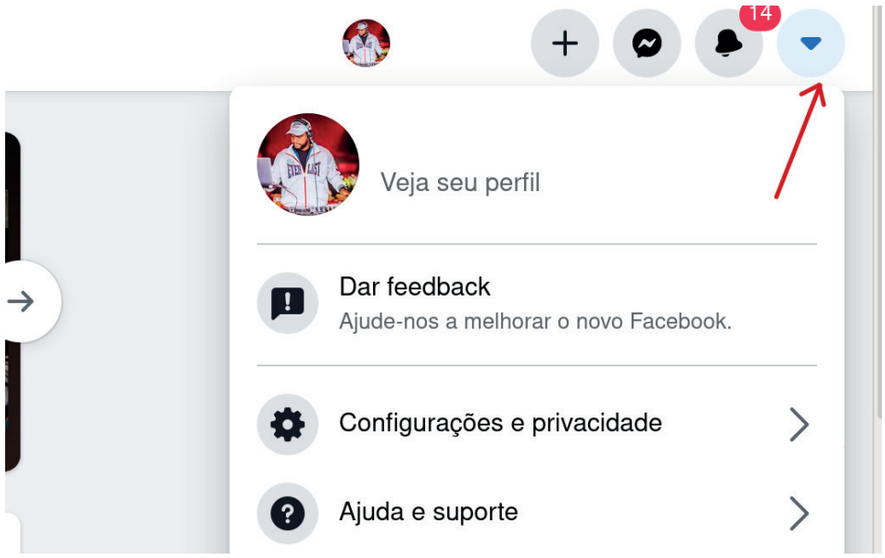
**4)** No lado direito desta tela você encontrará o menu **O que você pode fazer**.


**5)** Clique em **Gerenciar sua atividade fora do Facebook**. Uma janela mais detalhada será aberta.

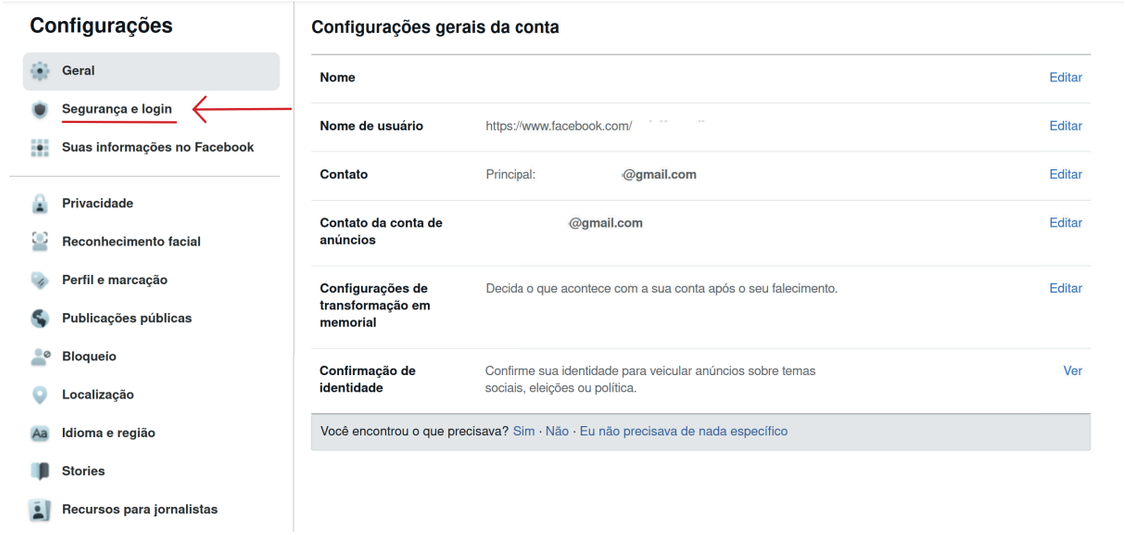
Como mostra a figura na página ao lado, nesta conta são 605 aplicativos e sites que enviam informações para o Facebook. Clique no botão **Desconectar histórico**. Na próxima janela, confirme pressionando o botão **Desconectar histórico**.

## 11.2 Confirmar quais computadores estão conectados em sua conta

**1)** Depois de logado em sua conta, siga até o menu localizado no canto superior direito e clique no ícone. Quando aparecerem as opções, clique em **Configurações e privacidade**.




**2)** Na tela **Configurações**, clique em **Segurança e login**.



# 11. Configurando e ajustando sua privacidade nas Redes Sociais

**3)** Na tela **Segurança e Login**, será possível você confirmar quais dispositivos estão conectados à sua conta do Facebook. Caso não reconheça algum, clique no local indicado na figura e selecione **Sair**.

# 12. Ativando a autenticação de dois fatores em Redes Sociais

A autenticação de dois fatores é um recurso de segurança que ajuda a proteger sua conta de alguns serviços na Internet, inclusive suas Redes Sociais. Com este recurso habilitado, você estará mais seguro contra ataques de sequestro e de invasão de sua conta.

Na autenticação de dois fatores, também conhecido como duas etapas, quando você for realizar o login em sua conta, o aplicativo irá solicitar que você insira um código enviado por SMS ou por meio de outro aplicativo de autenticação de ID. Este recurso vai evitar que outras pessoas tentem logar na conta, já que não terão o código que será enviado a você.

Agora, vamos conhecer os passos para habilitar este recurso em alguns aplicativos:

## 12.1 Facebook

**1)** Depois de logado em sua conta, siga até o menu localizado no canto superior direito e clique no ícone. Quando aparecerem as opções, clique em **Configurações e privacidade**.

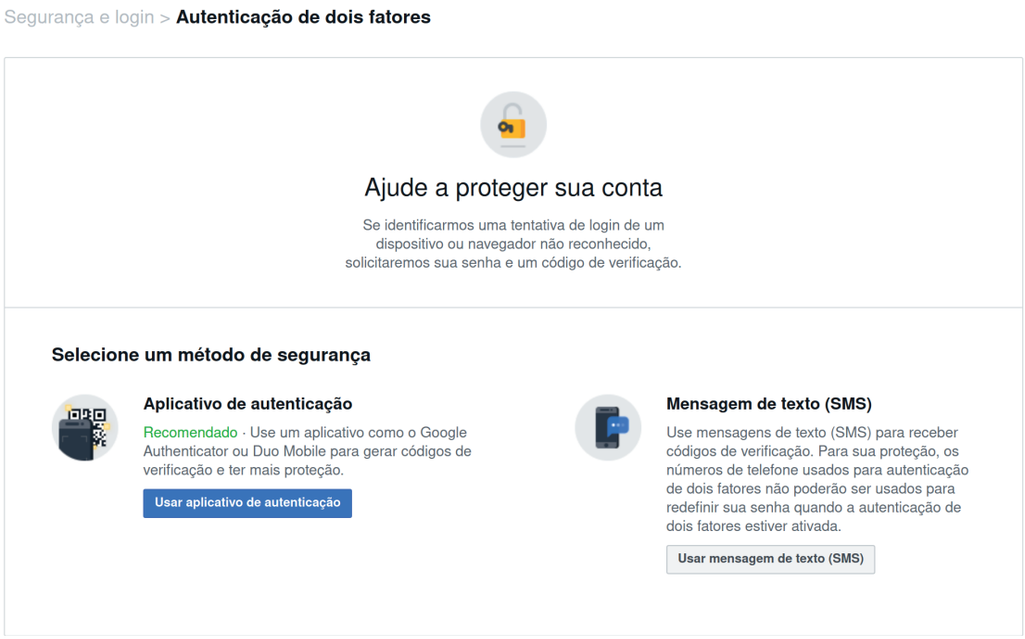
# 12. Ativando a autenticação de dois fatores em Redes Sociais

**2)** Clique na opção **Configurações.**


**3)** Role a tela para baixo até **Usar autenticação de dois fatores** e clique em **Editar**.

# 12. Ativando a autenticação de dois fatores em Redes Sociais

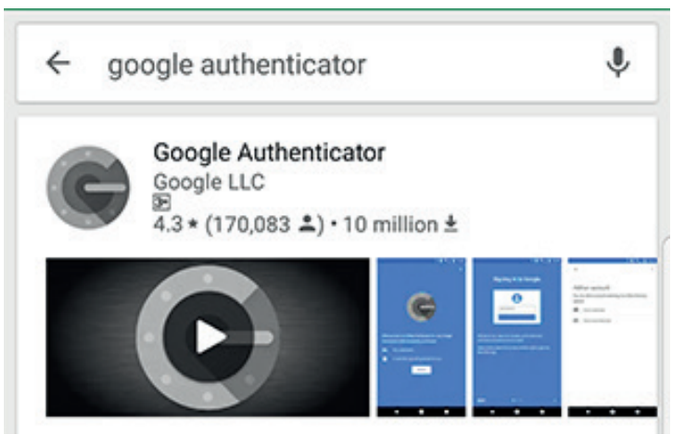
**4)** Escolha o método de segurança que deseja adicionar e siga as instruções na tela.




Ao configurar a autenticação de dois fatores no Facebook, você precisará escolher um dos dois métodos de segurança:

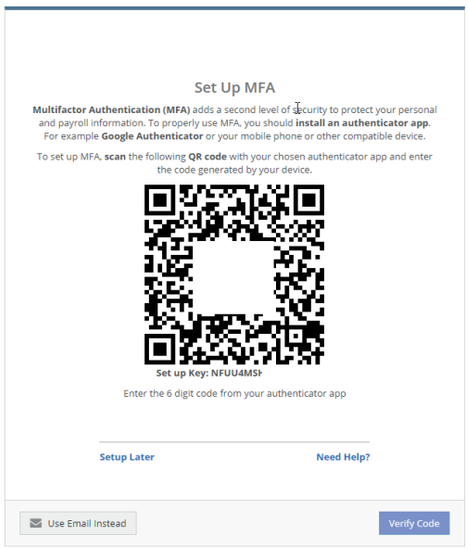
- **Códigos de login de um aplicativo de autenticação de terceiros**

Para esta opção, um aplicativo irá gerar um número aleatório (token) que, ao ser solicitado, você deverá digitar na tela de login do Facebook. Sugerimos a instalação do Google Authenticator, facilmente encontrado na Playstore.



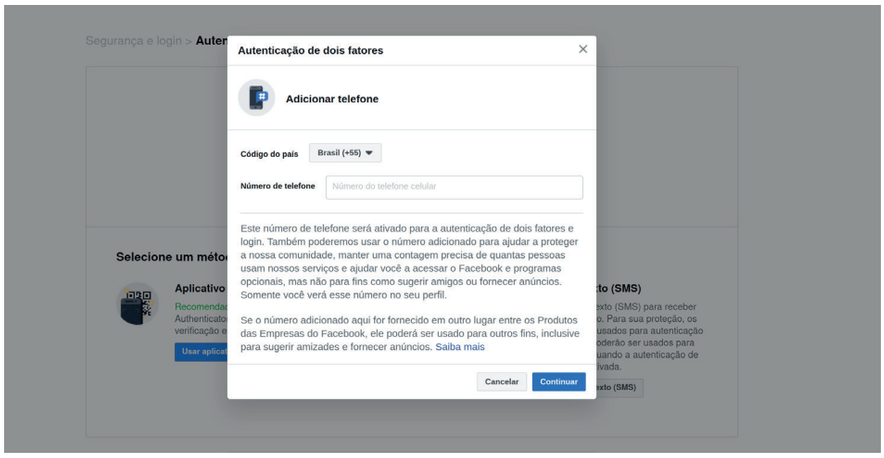
# 12. Ativando a autenticação de dois fatores em Redes Sociais

Ao selecionar a opção **Aplicativo de Autenticação**, uma tela com um QR Code será apresentada. Abra o aplicativo Google Authenticator em seu smartphone, clique no botão **Adicionar** e enquadre a câmera do equipamento na imagem idêntica à imagem abaixo.




## ■ Códigos de login de um aplicativo de autenticação de terceiros

Para esta opção, um aplicativo irá gerar um número aleatório (token) que, ao ser solicitado, você deverá digitar na tela de login do Facebook. Sugerimos a instalação do Google Authenticator, facilmente encontrado na Playstore.



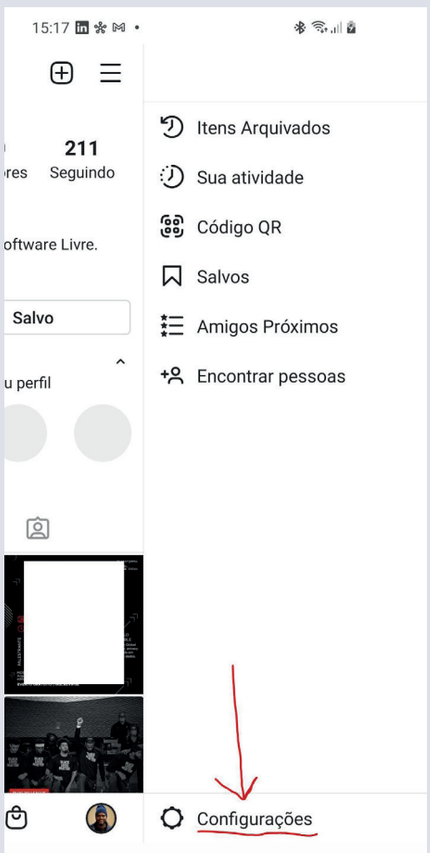
Contudo, caso você ainda não tenha divulgado seu número de telefone ao Facebook (geralmente eles sempre solicitam), dê preferência para usar a opção do Google Authenticator.

Atenção! **Não** clique na opção **Salvar este navegador** se você estiver usando um computador público ou corporativo que outras pessoas também usem. O Facebook precisa lembrar as informações do computador e navegador para que possa reconhecer você na próxima vez que entrar no site da Rede Social.

**Pronto! Sua conta está protegida com o duplo fator de autenticação!**

## 12.2 Instagram

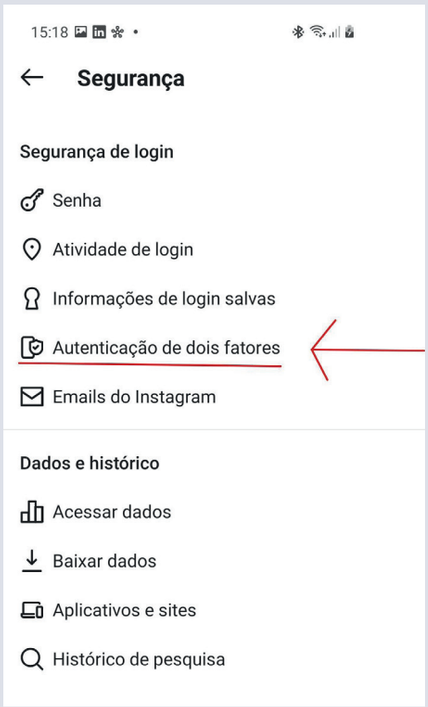
**1)** Abrir o aplicativo em seu smartphone e clicar no menu **Configurações**.




**2)** Na tela seguinte, clique em **Segurança**.

# 12. Ativando a autenticação de dois fatores em Redes Sociais

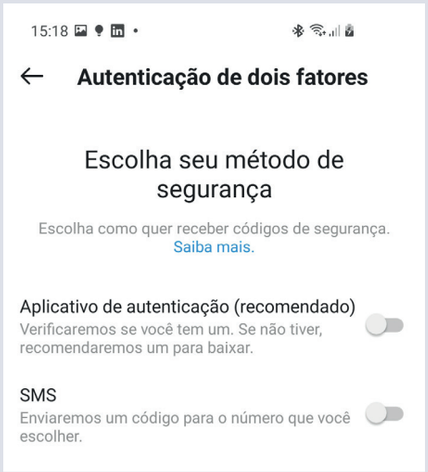
**3)** E depois em **Autenticação de dois fatores**.




**4)** Confirme se você já tem o aplicativo Google Authenticator instalado em seu smartphone e siga as orientações para os próximos passos. Clique em **Começar**.

# 12. Ativando a autenticação de dois fatores em Redes Sociais

**5)** Escolha a opção recomendada: **Aplicativo de Autenticação**. Esta escolha requer o Google Authenticator instalado.

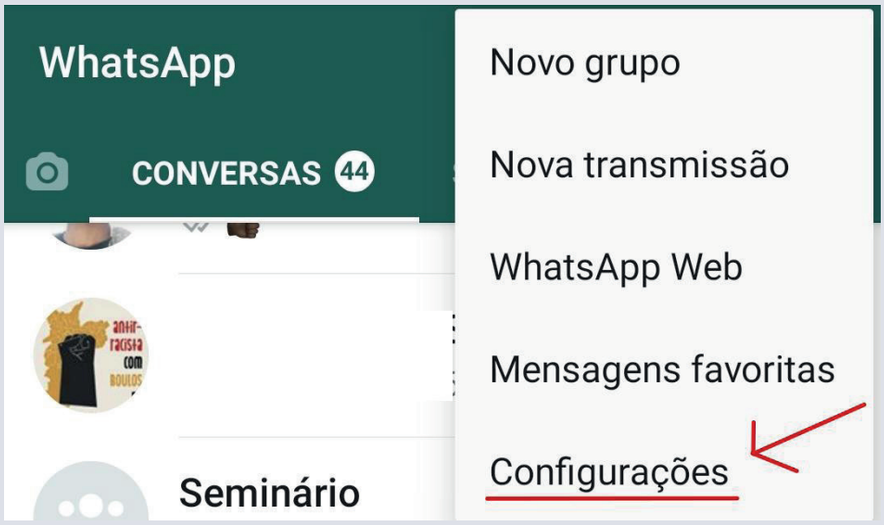



**6)** Clique em **Avançar** na próxima tela e siga as as orientações seguintes.


**7)** Se o Google Authenticator já estiver instalado em seu dispositivo, o próximo passo será a confirmação da inclusão da conta do Instagram. Clique em **Confirmar** e sua conta já estará protegida com o duplo fator de autenticação.

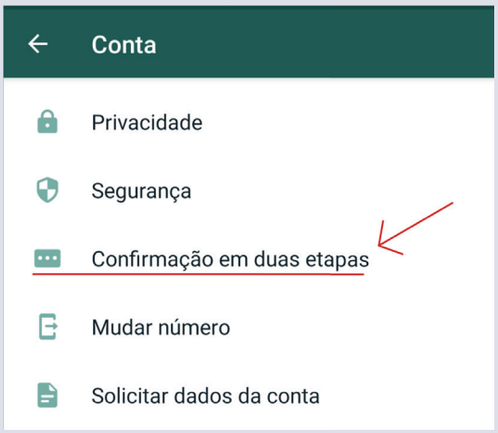
## 12.3 WhatsApp

**1)** Acesse o menu do WhatsApp e escolha a opção **Configurações**.




**2)** Na tela seguinte, selecione a opção **Conta**.

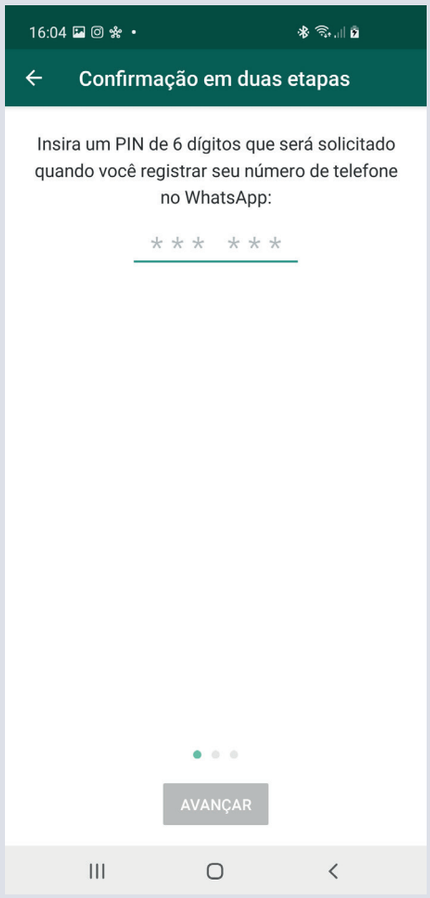

**3)** Na tela da opção Conta, clique em **Confirmação em duas etapas**.



# 12. Ativando a autenticação de dois fatores em Redes Sociais

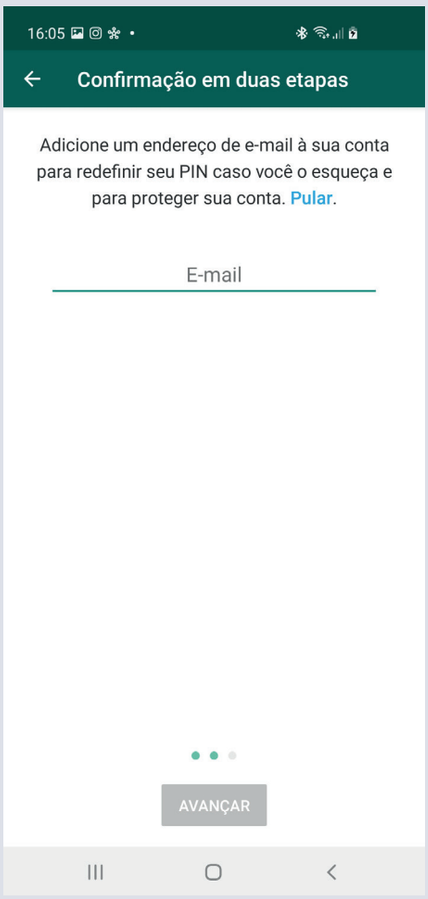
**4)** Siga as orientações e clique em **Ativar**.


**5)** A próxima tela irá solicitar uma senha de seis números. Este será o seu número de autenticação do WhatsApp e será solicitado em determinados momentos de seu uso.

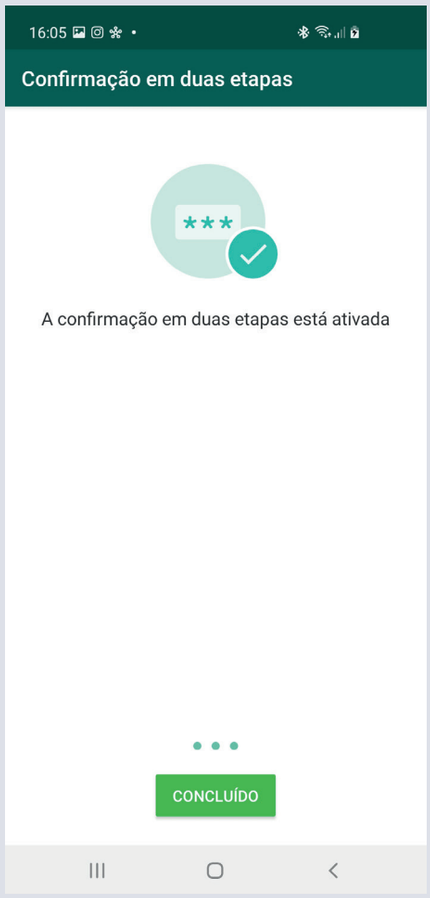


# 12. Ativando a autenticação de dois fatores em Redes Sociais

**6)** Depois de confirmar o número do PIN, será solicitado o cadastro de uma conta de e-mail. Este recurso irá garantir a redefinição de sua senha caso a esqueça.




**7)** Depois de confirmar o e-mail, sua conta estará protegida pelo processo de duas etapas.



# 13. Minha conta do WhatsApp foi hackeada, o que eu faço?

Por ser uma das redes com mais usuários, o WhatsApp acaba sendo uma das ferramentas mais visadas por cibercriminosos e fraudadores. Nunca forneça nenhum tipo de código e dados de sua conta caso receba alguma ligação ou mensagem.

Uma das formas mais utilizadas para hackear contas do WhatsApp é o fraudador entrar em contato telefônico e solicitar a sequência de números que será apresentada para você por meio de um SMS.

Caso você tenha caído em algum golpe e tiveram sucesso em hackear sua conta, envie uma mensagem explicando o ocorrido para o e-mail: support@whatsapp.com.

# 14. Outras dicas para a sua segurança nas Redes Sociais

ⓘ Caso deseje utilizar o recurso de geolocalização, procure fazer check-in apenas em locais movimentados e, de preferência, ao sair deles;

ⓘ Se alguém estiver assediando ou ameaçando você, remova-o de sua lista de amigos, bloqueie-o e denuncie-o ao administrador do site;

ⓘ Por razões de segurança pessoal, nunca revele a data e local de nascimento, endereço residencial ou número de telefone, pois isso pode colocá-lo em sério risco de roubo de identidade e fraude;

ⓘ No Twitter, Facebook e Instagram, desabilite a opção de que outras pessoas possam te marcar;

ⓘ Se você tiver aplicativos de Redes Sociais em seu telefone, certifique-se de proteger seu dispositivo com senha (conforme já apresentado neste Manual);

ⓘ **Tenha cuidado com amizades excessivas:** para você e sua atuação, pode ser muito importante ter o maior número de seguidores e amigos. Nós nos deparamos com amigos com milhares de seguidores, o que até mesmo pode nos despertar também o desejo de ter números expressivos. Um grande número de seguidores, entretanto, nem sempre é positivo. Alguns deles poderão ser perfis falsos, justamente para alimentar sistemas de vigilância e também introduzir spam na sua página. Antes de aceitar amigos desconhecidos, pesquise o perfil deles;

ⓘ Evite publicar sua localização por meio de comentários ou imagens, pois estas informações podem permitir ataques e perseguições;

ⓘ Certifique-se de que os membros de sua família tomem precauções semelhantes em relação a suas configurações de privacidade e de compartilhamento de dados pessoais;

# 14. Outras dicas para a sua segurança nas Redes Sociais

ⓘ Tenha cuidado ao encontrar seus novos amigos cibernéticos pessoalmente, afinal é difícil julgar as pessoas pelas fotos ou informações que postam sobre si mesmas. Se você decidir se encontrar com alguém pessoalmente, faça-o durante o dia em um lugar público e peça informações que você possa verificar, como o local de trabalho da pessoa;

ⓘ Não divulgue planos de viagens e nem por quanto tempo ficará ausente da sua residência.

# 15. Glossário

**Antimalware** – Programa que procura detectar e remover os códigos maliciosos de um dispositivo.

**Atacante** – Responsável pela realização de um ataque cibernético.

**Brute force (força bruta)** – Consiste em uma tentativa de violar uma senha ou um nome de usuário, usando uma abordagem de "tentativa e erro" e esperando que, em algum momento, seja possível adivinhá-la.

**Código malicioso** – Programas que executam ações e/ou atividades maliciosas em um dispositivo.

**Criptografia** – É o processo de pegar uma mensagem ou um arquivo e, por meio de uma chave e algumas operações matemáticas, transformá-los em mensagens e arquivos inteligíveis (embaralhados). Estas mensagens e arquivos "criptografados" só poderão voltar ao seu estado "normal" a partir do uso da chave e das operações matemáticas usadas inicialmente.

**Keylogger** – É um tipo específico de spyware. Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador.

**Malware** – É um termo genérico utilizado para denominar qualquer tipo de código/programa malicioso. Inclui: vírus, worms, spywares, trojans, backdoors, rootkits, keyloggers, entre outros.

**Phishing** – É um tipo de atividade que tem o objetivo de enganar as pessoas para que compartilhem informações confidenciais, como senhas e número de cartões de crédito. É uma das técnicas mais utilizadas por fraudadores e geralmente a sua proliferação é feita por meio de mensagens enviadas com promoções através de SMS, mensagens no WhatsApp e e-mails.

**Ransomware** – É um tipo de ataque por meio de código malicioso criado com o objetivo de criptografar os arquivos de um computador para liberá-los após o pagamento de um valor.

# 14. Glossário

**Rootkit** – Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

**Spam** – Termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

**Spyware** – Tipo específico de código malicioso. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

**Trojan (cavalo de troia)** – É um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, sem o conhecimento do usuário, tais como furto de senhas, de números de cartões de crédito e outras informações pessoais, e também inclusão de backdoors.

**Vírus** – Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

**Worm** – São códigos maliciosos que se espalham automaticamente pela rede de computadores sem que sejam percebidos. Um worm pode realizar ações perigosas, como consumir banda de rede e recursos locais, causando sobrecarga dos servidores ou da rede e indisponibilidade dos serviços.

# Direção Executiva da CUT (2019/2023)

**Presidente**
Sérgio Nobre

**Vice-Presidente**
Vagner Freitas

**Secretária-Geral**
Carmen Helena Ferreira Foro

**Secretário-Geral Adjunto**
Aparecido Donizeti da Silva

**Secretário de Administração e Finanças**
Ariovaldo de Camargo

**Secretária-Adjunto de Administração e Finanças**
Maria Aparecida Faria

**Secretário de Relações Internacionais**
Antonio de Lisboa Amâncio Vale

**Secretário-Adjunto de Relações Internacionais**
Quintino Marques Severo

**Secretário de Assuntos Jurídicos**
Valeir Ertle

**Secretário de Comunicação**
Roni Anderson Barbosa

**Secretário-Adjunto de Comunicação**
Admirson Medeiros Ferro Junior (Greg)

**Secretário de Cultura**
José Celestino (Tino)

**Secretário-Adjunto de Cultura**
Eduardo Lírio Guterra

**Secretária de Formação**
Rosane Bertotti

**Secretária-Adjunta de Formação**
Sueli Veiga de Melo

**Secretária de Juventude**
Cristiana Paiva Gomes

**Secretário de Relações de Trabalho**
Ari Aloraldo do Nascimento

# Direção Executiva da CUT (2019/2023)

**Secretária-Adjunta de Relações de Trabalho**
Amanda Gomes Corsino

**Secretária da Mulher Trabalhadora**
Junéia Batista

**Secretária de Saúde do Trabalhador**
Madalena Margarida da Silva Teixeira

**Secretária-Adjunta de Saúde do Trabalhador**
Maria de Fátima Veloso Cunha

**Secretária de Meio Ambiente**
Daniel Gaio

**Secretária de Mobilização e Movimentos Sociais**
Janeslei Albuquerque

**Secretária de Políticas Sociais e Direitos Humanos**
Jandyra Uehara

**Secretária de Combate ao Racismo**
Anatalina Lourenço

**Secretária-Adjunta de Combate ao Racismo**
Rosana Sousa Fernandes

**Secretária de Organização e Política Sindical**
Maria das Graças Costa

**Secretário-Adjunto de Organização e Política Sindical**
Jorge de Farias Patrocínio

**Diretores Executivos**

Aline Marques
Ângela Maria de Melo
Claudio Augustin
Cláudio da Silva Gomes
Francisca Trajano dos Santos
Ismael José Cesar
Ivonete Alves
João Batista (Joãozinho)
José de Ribamar Barroso
Juvândia Moreira Leite
Marcelo Fiorio
Marcelo Rodrigues
Mara Feltes
Maria Josana de Lima
Maria Julia Nogueira
Marize Souza Carvalho
Milton dos Santos Rezende
Pedro Armengol
Rogério Pantoja
Sandra Regina Santos Bitencourt
Virginia Berriel
Vitor Carvalho

www.cut.org.br
facebook.com/cutbrasil
www.instagram.com/cutbrasil/
twitter.com/cut_brasil
www.youtube.com/cutbrasil
soundcloud.com/cutbrasil

CUT BRASIL
CENTRAL ÚNICA DOS TRABALHADORES

Apoio

SOLIDARITY CENTER
AFL-CIO