

# *Guia para Uso Seguro de Serviços e Aplicativos Digitais*



# Índice

- Introdução
- Vazamento de Dados e Privacidade
- Engenharia Social e Fraudes
- Roubo de Identidade
- Malware e Ataques Cibernéticos
- Golpes Financeiros e Falsos Investimentos
- Impacto Reputacional e Assédio
- O Que Fazer em Caso de Incidentes
- Anexos

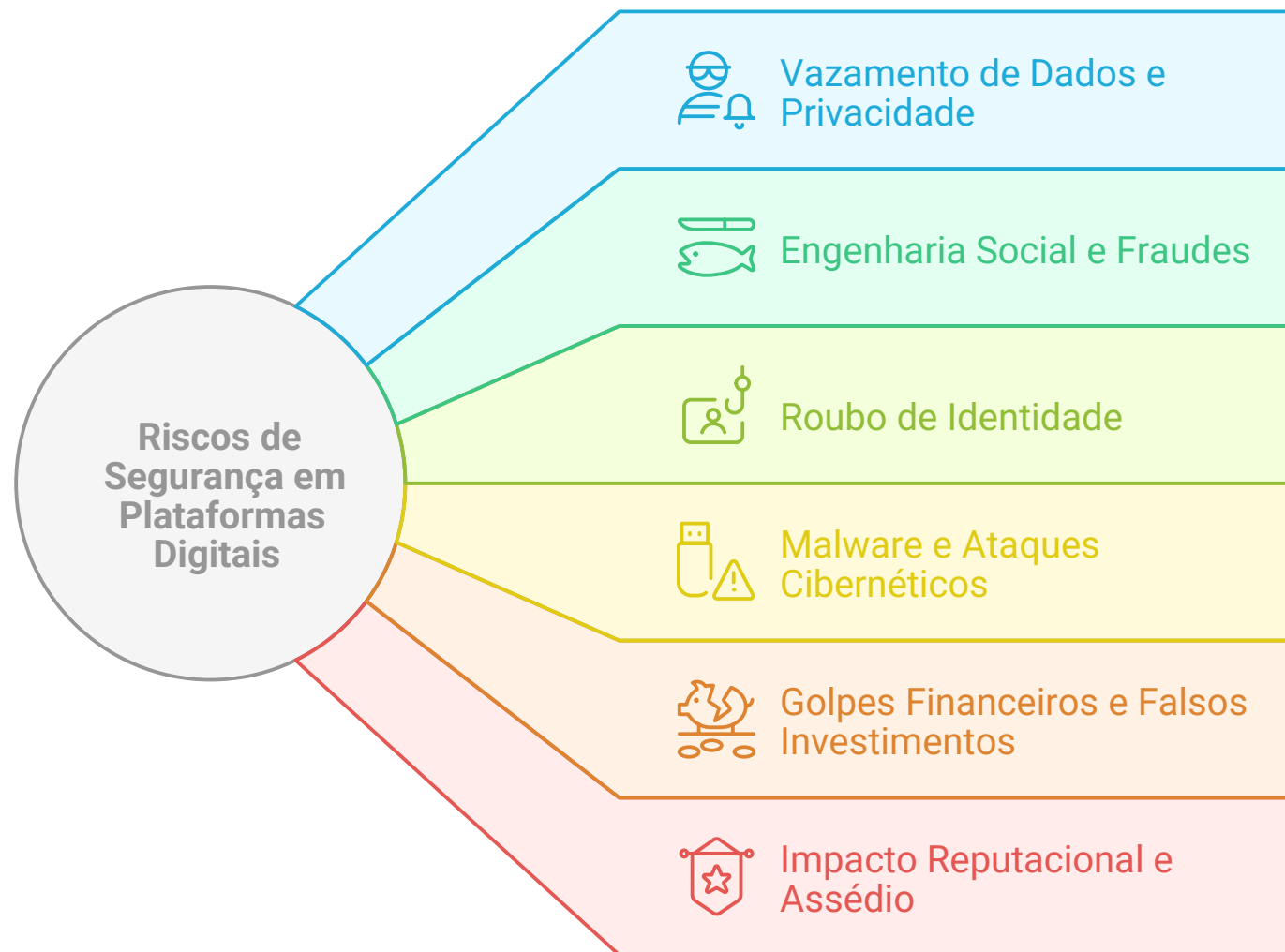
- O Grupo Energisa não se responsabiliza pela perda de dados pessoais após a execução por parte do usuário nas orientações relacionadas neste guia.

## Introdução

Hoje em dia, usamos a internet para quase tudo: conversar com amigos, pagar contas, assistir vídeos e muito mais. Mas, junto com essas facilidades, existem riscos como golpes, roubo de dados e ataques virtuais.

Este guia traz dicas simples para você se proteger e usar a internet com segurança.

**Para saber como aplicá-las na prática, clique nos links indicados no material ou consulte os anexos.**



## Vazamento de Dados e Privacidade

Ocorre quando suas informações pessoais (como nome, CPF, telefone) são expostas na internet sem sua autorização. Isso pode acontecer por falhas nos aplicativos ou quando você mesmo compartilha dados sem perceber. Dados vazados podem ser usados para fraudes, roubo de identidade e ataques direcionados.

### Como me Proteger?



#### Principais Controles Tecnológicos Associados

- Ativar login biométrico (impressão digital/Face ID)



- Desativar compartilhamento de localização em tempo real



- Cadastrar um canal seguro para recuperação de senhas



Consulte “Mais Controles” clicando nos links abaixo e saiba “Como Aplicá-los” na prática em:



REDES SOCIAIS



APPS DE MENSAGENS



APPS BANCÁRIOS



CONTAS DE E-MAIL



SISTEMAS OPERACIONAIS



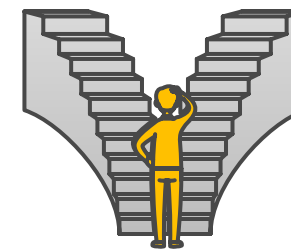
## Cuidados Pessoais

### O QUE FAZER?

- ✓ Use senhas seguras e únicas para cada conta
- ✓ Mantenha seus perfis restrito para amigos ou contatos conhecidos
- ✓ Atualize regularmente os contatos de recuperação
- ✓ Revise permissões de apps regularmente.
- ✓ Verifique periodicamente os dispositivos vinculados.

### O QUE NÃO FAZER?

- ⊗ Não salve informações sensíveis permanentemente
- ⊗ Não divulgue sua localização nas redes sociais
- ⊗ Não manter aplicativos não utilizados instalados.
- ⊗ Não permitir que informações privadas apareçam nas notificações.
- ⊗ Não interagir com pessoas desconhecidas ou sem verificação.





## Engenharia Social e Fraudes

Engenharia social envolve manipulação psicológica para convencer usuários a revelarem informações confidenciais. Golpistas podem se passar por bancos, empresas ou até amigos e familiares para enganar você e roubar suas informações.

### Como me Proteger?

#### Proteção contra E-mails Indesejados

Ativar filtros para bloquear mensagens de spam e tentativas de fraude (phishing),

#### Confirmação de Pagamento

Ativar "confirmação antes de envio" de pagamentos

#### Alertas Suspeitos

Ativar alerta de atividade suspeita na conta

#### Bloqueio Preventivo

Habilitar o bloqueio de chamadas e mensagens desconhecidas

Acesse os guias de cada tipo de plataforma e saiba **COMO APLICAR** esses controles:



## Práticas Recomendadas

### O que fazer?

- ✓ Revisar os dados antes de confirmar qualquer transação.
- ✓ Relatar tentativas de golpes às plataformas.
- ✓ Evitar responder números desconhecidos.

### O que não fazer?

- ✗ Não clicar em links suspeitos recebidos por e-mail ou mensagens.
- ✗ Não fornecer informações pessoais em chamadas ou mensagens suspeitas.



# Roubo de Identidade

Roubo de identidade quando alguém não autorizado usa suas informações para abrir contas, fazer compras ou cometer fraudes em seu nome. Isso pode acontecer através de vazamentos de dados ou uso de informações pessoais suas quando compartilhadas online.

## Como me proteger?



Consulte "Mais Controles" clicando nos links abaixo e saiba "Como Aplicá-los" na prática em:



REDES SOCIAIS



APPS DE MENSAGENS



APPS BANCÁRIOS



CONTAS DE E-MAIL



SISTEMAS OPERACIONAIS

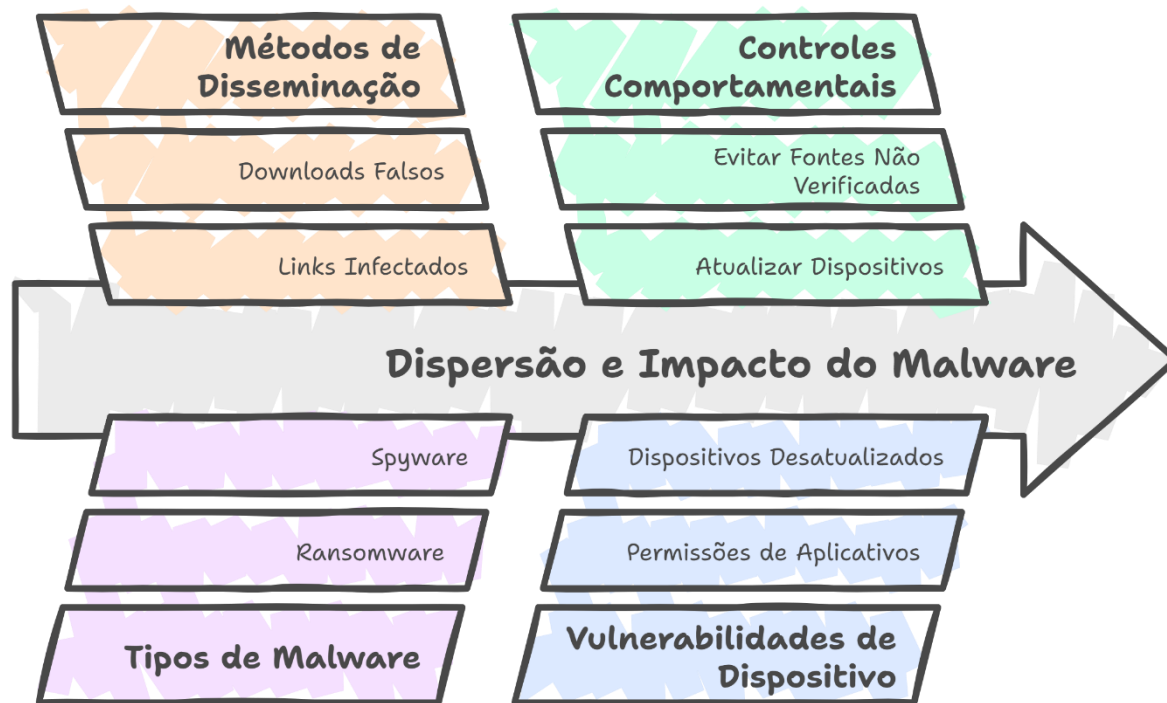
## Controles Comportamentais Importantes



## Malware e Ataques Cibernéticos

Malwares são programas maliciosos que podem roubar informações, travar seu dispositivo ou até pedir resgate pelos seus dados. Eles são disseminados através de links infectados, downloads falsos e anexos suspeitos.

### Compreendendo Melhor:



### Controles Tecnológicos



Consulte “Mais Controles” clicando nos links abaixo e saiba “Como Aplicá-los” na prática em:



## Golpes Financeiros e Falsos Investimentos

Golpes financeiros incluem fraudes bancárias, promessas de retornos irreais em investimentos e falsas promoções. Muitos criminosos usam redes sociais, e-mails e sites falsos para disseminar esses golpes.

Consulte "Mais Controles" e saiba "Como Aplicá-los" na prática em:



### Cuidados com Informações Financeiras

- Nunca compartilhe dados financeiros em mensagens privadas ou ligações recebidas.
- Use cartões virtuais para compras online, reduzindo o risco de fraudes.
- Ative alertas de movimentações financeiras para detectar possíveis acessos indevidos.

#### Lembre-se:

*"Nunca divulgue informações financeiras, especialmente em redes sociais."*

Use apenas aplicativos bancários oficiais



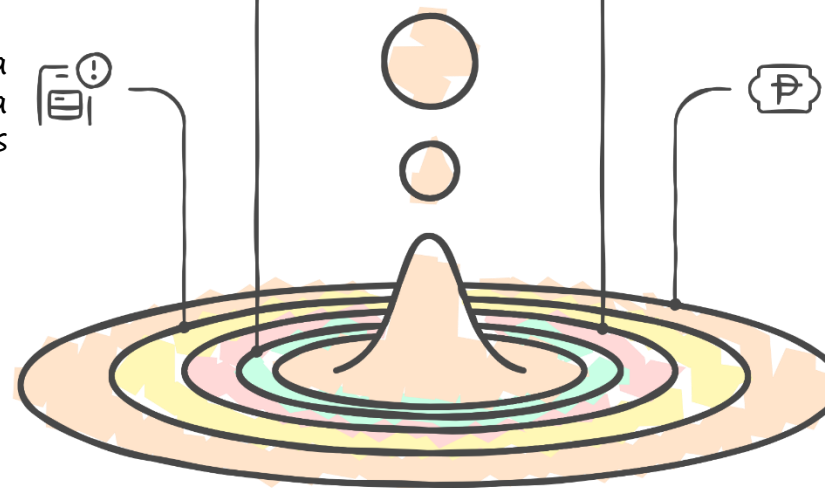
Nunca faça pagamentos para desconhecidos



Garanta que suas senhas não sejam salvas automaticamente



Desconfie de promessas de lucros fáceis



### Controles Tecnológicos

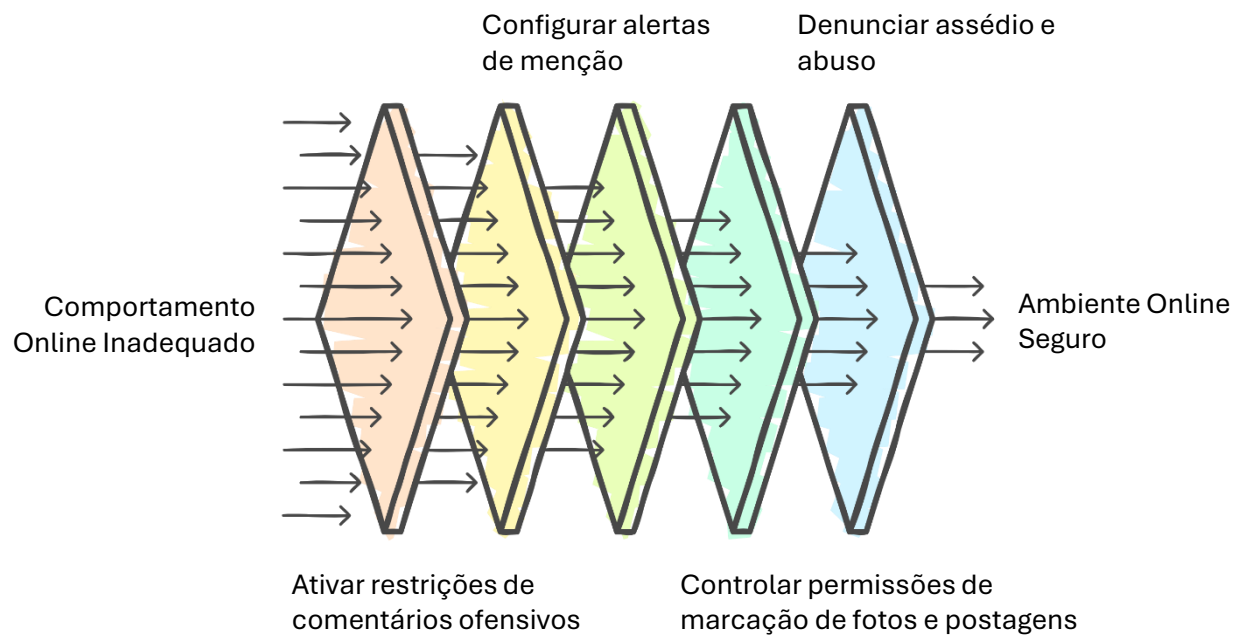




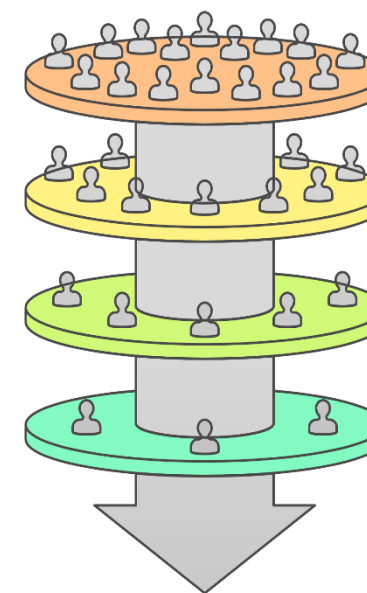
## Impacto Reputacional e Assédio

Postagens e mensagens inadequadas podem afetar sua reputação profissional e pessoal. Além disso, o assédio online também é um problema crescente e necessitam de prevenção e denúncia.

### Boas Práticas de Comportamento Online



### Proteja-se!



- Bloqueie usuários com comportamento inadequado
- Denuncie conteúdos ofensivos nas redes sociais
- Não participe de discussões ofensivas
- Pense antes de postar algo que pode comprometer sua imagem

Saiba "Como Aplicar" essas práticas em:



## Sua conta foi invadida?

1. **Tente recuperar o acesso** imediatamente redefinindo a senha:
  - No **WhatsApp**: Vá para Configurações > Conta > Verificação em duas etapas e redefina o PIN.
  - No **Instagram/Facebook**: Acesse a opção Esqueci minha senha na tela de login e siga as instruções.
2. **Revise e encerre sessões suspeitas**:
  - No **Instagram/Facebook**: Vá para Configurações e privacidade > Segurança e login e remova dispositivos desconhecidos.
  - No **WhatsApp**: Se notar acessos não autorizados, saia de todas as sessões do WhatsApp Web e reative a verificação em duas etapas.
3. **Ative a verificação em duas etapas (MFA)** caso ainda não tenha feito.
4. **Verifique e atualize suas informações de recuperação**, como e-mail e número de telefone, para evitar futuras invasões.
5. **Se não conseguir recuperar a conta**, entre em contato com o suporte da plataforma para solicitar a recuperação.

## Caiu em um golpe?

1. **Se fez um pagamento ou compartilhou dados bancários**, entre em contato com seu banco imediatamente para tentar reverter a transação e bloquear possíveis fraudes.
2. **Denuncie à plataforma** onde ocorreu o golpe:
  - No **Instagram/Facebook**: Acesse a postagem ou perfil fraudulento, toque nos três pontos : e selecione Denunciar.
  - No **WhatsApp**: Acesse a conversa do golpista, toque no nome e selecione Denunciar e bloquear.
3. **Registre um boletim de ocorrência online** no site da Polícia Civil do seu estado, especialmente se envolver transações financeiras ou roubo de identidade.
4. **Se forneceu informações sensíveis (CPF, RG, senhas)**, monitore seu nome em serviços de proteção contra fraudes, como **Registrato (Banco Central)** e **Serasa**.

## Detectou um perfil falso?

1. **Denuncie diretamente na plataforma**:
    - No **Instagram/Facebook**: Acesse o perfil falso, toque em : e selecione Denunciar > Imitação de outra pessoa.
    - No **WhatsApp**: Informe aos seus contatos que alguém pode estar se passando por você e peça para que também denunciem.
  2. **Avise seus amigos e familiares**, pois o perfil falso pode estar tentando enganar conhecidos.
  3. **Se a conta falsa estiver se passando por uma empresa**, verifique se a empresa já possui um canal oficial para denúncias e faça um alerta público sobre perfis fraudulentos.
- ✓ **Dica Extra**: Se sua foto de perfil estiver sendo usada sem autorização, você pode reivindicar seus direitos sobre a imagem.



































✦ **Lembre-se**: Quanto mais rápido agir, menor o impacto do incidente. Denunciar atividades suspeitas ajuda a tornar as redes sociais mais seguras para todos.

Obrigado!



## Redes Sociais

(Clique nas imagens de “👉” para acessar o passo a passo de como implementar o controle indicado em cada plataforma.)

Controles de Segurança	Tiktok	LinkedIn	Facebook	Instagram	Youtube
Cadastrar um canal seguro para recuperação de senhas.	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>
Habilitar o duplo fator de autenticação.	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>
Habilitar o modo privado para a rede social, sendo necessário aceitar seguidores ou amigos para visualizar informações do perfil.	<a href="#"></a>	X	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>
Habilitar alertas para tentativas de login a partir de dispositivos ou locais desconhecidos.	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>
Remover acessos de aplicativos de terceiros que não são mais utilizados.	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>
Definir níveis adequados de privacidade para publicações e informações do perfil.	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>
Revisar e desconectar sessões ativas em dispositivos que não são mais utilizados ou que possam estar comprometidos.	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>	<a href="#"></a>

 Apps de Mensagens

Controles de Segurança	WhatsApp	Telegram
<b>Ativar as notificações de segurança no smartphone principal.</b>	Acesse Configurações > Conta > Ative "Mostrar notificações de segurança"	Acesse Configurações > Notificações e Sons > Certifique-se de que as notificações relevantes estão ativadas
<b>Crie uma chave de acesso para proteção da conta.</b>	Acesse Configurações > Conta > Chave de Acesso > Definir uma senha	Acesse Configurações > Privacidade e Segurança > Senha de Bloqueio > Ativar e definir uma senha
<b>Confirme o endereço de e-mail atribuído à sua conta.</b>	Acesse Configurações > Conta > Endereço de email > Adicione ou atualize o e-mail cadastrado	Acesse Configurações > Privacidade e Segurança > Verificação em duas etapas > Verificar e-mail de recuperação
<b>Habilite a confirmação em duas etapas para adicionar mais uma camada de segurança no acesso a conta.</b>	Acesse Configurações > Conta > Verificação em duas etapas > Ativar e definir um código PIN	Acesse Configurações > Privacidade e Segurança > Verificação em duas etapas > Ativar e definir uma senha
<b>Habilite o bloqueio do App para solicitar uma senha / biometria para abrir o aplicativo.</b>	Acesse Configurações > Privacidade > Bloqueio do app > Ativar e configurar	Acesse Configurações > Privacidade e Segurança > Código de Bloqueio > Ativar e definir uma senha
<b>Permita que somente contatos possam ver a sua foto do Perfil.</b>	Acesse Configurações > Privacidade > Foto do perfil > Selecione "Meus contatos"	Acesse Configurações > Privacidade e Segurança > Foto do perfil > Escolha "Meus contatos"
<b>Permita que apenas seus contatos possam adicioná-lo em grupos.</b>	Acesse Configurações > Privacidade > Grupos > Escolha "Meus contatos"	Acesse Configurações > Privacidade e Segurança > Convites > Selecione "Meus contatos"
<b>Selecione "Ninguém" para que seus contatos não possam ver seus dados de Pix.</b>	Acesse Configurações > Privacidade > Pix > Escolha "Ninguém"	X
<b>Selecione "ninguém" ou "meus contatos" para que possam ver seu número de telefone</b>	X	Acesse Configurações > Privacidade e Segurança > Número de telefone > Escolha "Meus contatos" ou "Ninguém"
<b>Selecione "meus contatos" para garantir que somente seus contatos possam enviar convites.</b>	X	Acesse Configurações > Privacidade e Segurança > Convites > Escolha "Meus contatos"
<b>Verifique os dispositivos conectados à conta e mantenha somente os dispositivos confiáveis.</b>	Clique nos três pontinhos no canto superior direito da tela > Dispositivos conectados > Remova dispositivos desconhecidos	Acesse Configurações > Dispositivos > Verifique e remova conexões suspeitas



## Apps Bancários

(Clique nas imagens de “👉” para acessar o passo a passo de como implementar o controle indicado em cada plataforma.)

Controles de Segurança	Santander	Itaú	Nubank	Bradesco
Confirme as informações cadastradas no Perfil e verifique a existência de um canal seguro registrado para recuperação de senhas.	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>
Ative os alertas e notificações de compras por cartão para receber avisos por push.	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>
Altere o limite do seu pix para pagamentos e transferências, evitando que valores altos possam ser transferidos de uma única vez.	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>
Ative o Alô Protegido, proteção para que o aplicativo ajude a evitar golpes de falsas centrais.	X	X	<a href="#"><u>👉</u></a>	X



## Contas de E-mail

(Clique nas imagens de “👉” para acessar o passo a passo de como implementar o controle indicado em cada plataforma.)

Controles de Segurança	Outlook	Gmail	Yahoo	iCloud
Cadastrar um canal seguro (e-mail secundário e telefone válido para SMS) para recuperação de senhas.	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>
Habilitar o duplo fator de autenticação.	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>
Utilizar um app Autenticador (ex.: Microsoft Authenticator, Google Authenticator) para iniciar sessão sem necessidade de senha	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>
Garantir que somente dispositivos conhecidos estão vinculados à sua conta de e-mail	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>
(!) Ativar a Proteção Avançada do Google	X	<a href="#"><u>👉</u></a>	X	X
(!!) Ativar Proteção Avançada de Dados do iCloud	X	X	X	<a href="#"><u>👉</u></a>
Garantir que apenas aplicações e serviços conhecidos têm acesso às informações de e-mail	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>	<a href="#"><u>👉</u></a>

**Atenção:** Controles de segurança mais robustos requerem cuidados extras:

(!) Se você perder sua conta, a recuperação vai exigir etapas extras. Esta proteção conta com restrições como: Chave de acesso ou de segurança para login em novos dispositivos e restrição do uso da sua conta google em apps e serviços que exigirem acesso a dados sensíveis, como e-mails e dados do Google Drive.

(!!) Se você ativar a Proteção Avançada de Dados e perder o acesso à conta, a Apple não terá as chaves de criptografia para você recuperá-la. Desta forma, será necessário usar o código de acesso ou a senha do dispositivo, um contato de recuperação ou uma chave reserva pessoal.



## Sistemas Operacionais

Controles de Segurança	Android	iOS
<b>Habilite o bloqueio de tela e defina um código de acesso para criar uma barreira de segurança que impeça uma pessoa não autorizada de acessar seu smartphone.</b>	Abra o aplicativo "Configurações" > "Segurança" > "Bloqueio de tela". Escolha o tipo de bloqueio desejado (PIN, padrão, senha) e siga as instruções para configurá-lo.	Acesse "Ajustes" > "Face ID e Código" (ou "Touch ID e Código" em modelos anteriores) > "Ativar Código". Siga as instruções para definir um código de acesso.
<b>Use o Reconhecimento Facial para desbloquear o smartphone, autorizar compras e pagamentos e, iniciar uma sessão em vários apps de terceiros com segurança</b>	A disponibilidade do reconhecimento facial varia conforme o dispositivo. Em dispositivos compatíveis, vá para "Configurações" > "Segurança" > "Desbloqueio facial" e siga as instruções para configurar.	Acesse "Ajustes" > "Face ID e Código" > "Configurar Face ID". Siga as instruções para configurar o Face ID. Para autorizar compras, ative "iTunes e App Store" na mesma seção.
<b>Ative a função de Buscar Dispositivo para ajudar a encontrar o seu aparelho e impedir que outra pessoa ative ou use o smartphone.</b>	Abra "Configurações" > "Segurança" > "Encontrar Meu Dispositivo" e ative a opção.	Acesse "Ajustes" > toque no seu nome > "Buscar" > "Buscar iPhone" e ative a opção.
<b>Desative o conteúdo de notificações na tela de bloqueio, para que não sejam exibidas publicamente informações de recuperação de senha, tokens e códigos de validação</b>	Vá para "Configurações" > "Aplicativos e notificações" > "Notificações" > "Na tela de bloqueio" e escolha "Não mostrar notificações" ou "Ocultar conteúdo confidencial".	Acesse "Ajustes" > "Notificações" > "Mostrar Pré-visualizações" e selecione "Quando Desbloqueado" ou "Nunca".
<b>Controle o acesso a informações em apps e as informações de localização compartilhadas.</b>	Vá para "Configurações" > "Privacidade" > "Gerenciador de permissões" e selecione categorias como "Localização", "Contatos", "Câmera" etc., para ajustar as permissões dos aplicativos.	Acesse "Ajustes" > "Privacidade" e selecione categorias como "Serviços de Localização", "Contatos", "Fotos" etc., para gerenciar as permissões de cada aplicativo.
<b>Crie senhas fortes e proteja a conta com multifator de autenticação (MFA) para manter a sua conta segura</b>	Utilize aplicativos de autenticação, como o Google Authenticator ou o Microsoft Authenticator, disponíveis na App Store e Google Play Store, para configurar a autenticação de dois fatores em suas contas.	
<b>Proteja os seu dados caso ocorra perda ou roubo do seu smartphone utilizando o Modo Perdido (iOS) / Bloqueio Remoto (Android): Permite bloquear o dispositivo remotamente e exibir uma mensagem de contato caso o aparelho seja perdido.</b>	Acesse "android.com/find", faça login com sua conta Google, selecione o dispositivo perdido e escolha a opção "Bloquear" para bloquear remotamente e adicionar uma mensagem de contato.	Acesse o site "iCloud.com" ou use o app "Buscar" em outro dispositivo Apple, selecione seu iPhone perdido e ative o "Modo Perdido".
<b>Utilize o recurso "Bloqueio de Aplicativos" para bloquear os aplicativos indesejados.</b>	Como configurar a Pasta Segura no Samsung > Abra o app "Configurações" > Toque em "Biometria e Segurança" > Selecione "Private Share" > Faça login com a sua conta Samsung > Siga as instruções e defina um tipo de bloqueio para a Pasta Segura.	X
<b>Configure um PIN no cartão eSIM / chip do celular para exigir que um código de identificação seja inserido em um novo aparelho ou para fazer ligações e usar os dados celulares</b>	Vá para "Configurações" > "Segurança" > "Configurações do SIM" > "Bloqueio do cartão SIM" e ative a opção, inserindo um código PIN.	Acesse "Ajustes" > "Celular" > "PIN do SIM" e ative a opção, inserindo um código PIN.
<b>Tenha uma cópia de segurança das suas informações para restaurar em outro smartphone em caso de perda ou roubo.</b>	Ative o backup do Google. Vá para "Configurações" > "Sistema" > "Backup" e ative a opção "Fazer backup no Google Drive".	Utilize o iCloud para backups automáticos. Acesse "Ajustes" > toque no seu nome > "iCloud" > "Backup do iCloud" e ative a opção.
<b>Utilize o recurso "Recurso de Tempo de Uso" para impedir o acesso ao iCloud e bloquear os aplicativos indesejados, após determinado limite de tempo definido pelo usuário.</b>	X	Use o recurso "Tempo de Uso" para definir limites de uso para aplicativos específicos. Acesse "Ajustes" > "Tempo de Uso" > "Limites de Apps" e configure os limites desejados.
<b>Mantenha o seu dispositivo atualizado com as últimas versões do sistema operacional.</b>	Use o recurso "Bem-estar digital" para definir limites de uso de aplicativos. Vá para "Configurações"	Acesse "Ajustes" > "Tempo de Uso" e configure os limites desejados para aplicativos específicos ou categorias de aplicativos.