# Módulo 3: Navegação segura

Curso: Alfabetização Digital

COSAIC

2025

# Sumário

# Introdução

Neste módulo, você irá estudar o tema **[navegação segura]**, compreendendo seus conceitos fundamentais e aplicabilidades práticas. O objetivo é oferecer ao participante os conhecimentos necessários para *[utilizar a internet de forma segura, protegendo seus dados mais sensíveis.Além disso, também será abordado como agir em uma situação de furto/roubo do aparelho celular, de forma a ensinar medidas para amenizar os riscos de ter seus dados roubados.*

# 1. Senhas fortes

## 1.1. Por que é importante ter uma senha forte?

A senha é como uma chave que protege tudo que está dentro de uma conta: conversas, fotos, contas bancárias, redes sociais e outros dados pessoais. Quando a senha é fraca, golpistas e criminosos digitais podem invadir contas, acessar essas informações e até fazer compras em nome de outra pessoa. Uma senha forte ajuda a manter a privacidade e a segurança na internet.

## 1.2. Como criar uma senha segura?

Criar uma senha forte é fundamental para proteger as informações na internet. Uma senha segura precisa ser difícil de adivinhar, misturar letras maiusculas e minúsculas, números, símbolos (como @, !, &, %) e possuir no mínimo 8 caracteres.

Passo a passo para criar uma senha segura:

1. Crie uma senha que tenha significado para você.

   *Algo pessoal, fácil de lembrar, mas difícil de alguém adivinhar.*

2. Monte uma frase e utilize as primeiras letras de cada palavra da frase.

3. Inclua símbolos e números.

   *Substitua algumas letras por números ou símbolos que se pareçam com elas.*

4. Misture letras maiúsculas e minúsculas.

5. Verifique se tem mais de 8 caracteres.

Exemplo de senha :
Frase: “Minha casa tem 3 janelas e 1 porta!”
Senha: **Mct3j&1p!**
(9 caracteres)

Outra forma de montar uma senha segura:
Escolha uma palavra base e acrescente algo diferente em cada conta.
Exemplo:
**Abacax1@Gmail**
**Abacax1@Banco**

Exemplos de senhas fracas a serem evitadas:

- Usar sequências simples (ex.: 123456, abcdef)
- Usar palavras óbvias (ex.: senha123)
- Usar nomes próprios (ex.: Maria2024)
- Usar datas de nascimento (ex.: 01011990)

## 1.3. Onde guardar as senhas?

Guardar a senha com segurança é tão importante quanto criá-la.

Algumas opções seguras são:

- Anotar num caderno ou agenda guardada em local seguro.
- Criar códigos que só você entende.

Não recomendado:

- Fotos da senha no celular
- Anotar em papel solto
- Salvar no navegador do celular ou computador (como o Google Chrome)

## 1.4. Por que não salvar senhas no Google?

Quando o navegador pergunta "Deseja salvar esta senha?"e a pessoa aceita, a senha fica guardada no celular ou computador. Isso pode ser perigoso.

Riscos:

- Qualquer pessoa que usar o aparelho pode entrar nas contas, sem precisar da senha.
- Se o celular for roubado ou perdido, quem pegar pode acessar tudo que estiver salvo.
- Vírus ou aplicativos espiões podem roubar essas senhas salvas.

Alternativa segura:

- Não clicar em "Salvar senha".
- Anotar as senhas em local físico e seguro.
- Usar bloqueio de tela no celular (senha, digital ou desenho).

## 1.5. Quando trocar a senha?

Mesmo uma senha forte precisa ser trocada de tempos em tempos. É importante:

- Trocar se algo estranho acontecer (como mensagens enviadas sem a pessoa saber).
- Trocar se outra pessoa usou o seu celular ou computador.
- Trocar a cada 3 ou 6 meses, como forma de prevenção.

# 2. Verificação de Fake News e Golpes

## 2.1. O que é Fake News?

Fake News (em português, notícia falsa) é uma informação mentirosa ou enganosa que parece verdadeira, mas foi criada para enganar as pessoas, espalhar boatos, causar confusão ou até mesmo influenciar opiniões.

### 2.1.1 Por que a gente precisa se preocupar com com as Fake News?

- Notícias falsas e golpes digitais se espalham muito rápido.
- Pessoas de todas as idades e níveis de escolaridade podem vítimas.
- As Fake News podem ser um risco para nossa segurança física, mental e financeira.

### 2.1.2 Como as Fake News podem influenciar nossa vida?

As Fake News, ou notícias falsas, podem afetar diretamente o nosso dia a dia de várias formas, muitas vezes de maneira negativa. Veja alguns exemplos de como isso acontece: Notícias falsas que falam de curas milagrosas, dietas perigosas, remédios sem comprovação ou dicas de saúde que podem fazer mal.

**Exemplo:**
"Chá que curo o câncer em 3 dias!"
"Remédio caseiro que elimina a diabetes!"

**Por que são perigosas?**

- Podem fazer você abandonar um tratamento verdadeiro.
- Podem fazer você tomar substâncias perigosas.
- Podem causar pânico ou medo.
- Podem prejudicar outras pessoas se você compartilhar.

**Será que Isso é Verdade? Como Reconhecer Fake News na Saúde**

- A promessa é milagrosa?
- A notícia tem tom de urgência exagerada ?
- Tem erros protuguês?
- O link é estranho ou de site/origem desconhecida?
- Fala de um "estudo científico", mas não diz qual é?

## 2.2. Como saber se uma notícia é falsa (Fake News)?

Dicas simples:

- Leia além do título: manchetes chamativas podemm enganar
- Confira a data: notícias velhas podem voltar como se fossem novas
- Desconfie de exageros: ”cura milagrosa”, ”última chance”, ”todo mundo precisa saber”
- Verifique o site: É conhecido? Tem erros de português?

## 2.3. Como verificar se uma informação é confiável?

Ferramentas úteis:

**Google:** busque se outros sites sérios e confiáveis também falaram da notícia.
**Agências de checagem:**

- Lupa (https://lupa.uol.com.br/)
- Aos Fatos (https://aosfatos.org/])
- Fato ou Fake (https://g1.globo.com/fato-ou-fake/)

### 2.3.1 Dica de ouro:

Se ficou na dúvida, não compartilhe!

## 2.4. Golpes mais comuns na internet

Exemplos:

- Golpes do PIX: alguém finge ser parente pedindo dinheiro.
- Promoção falsa: ”ganhe um celular clicando aqui”.
- WhatsApp clonado: alguém se passa por você para pedir dinheiro
- Golpe do banco> SMS ou e-mail dizendo que sua conta foi(ou será) bloqueada.

Como se proteger:

- Nunca clique em links suspeitos
- Em caso de parente ou conhecido pedindo dinheiro por WhatsApp ou qualquer outra rede social, confirme com a pessoa por telefone ou vídeo se foi realmente ela que mandou aquela mensagem.
- Desconfie de urgência e pressão (”mande agora”, ”última chance”).

## 2.5. Golpes digitais: o que são e como não cair neles?

Golpe digital é quando alguém usa a internet, celular ou redes sociais para enganar pessoas e roubar dinheiro, dados ou informações pessoais.

Esses golpes podem acontecer por:

- Mensagens no WhatsApp ou SMS;
- Links falsos
- Sites de compras falsos
- Perfis falsos nas redes sociais
- Ligações telefônicas falsas.

O objetivo do golpista é enganar você para conseguir dinheiro, senhas ou acesso ao seu celular.

**Lembre-se:**

- Golpes digitais afetam pessoas de todas as idades e perfis.
- Informação é a melhor forma de se proteger.
- Está barato demais? Desconfie!

### 2.5.1 Como identificar propagandas falsas

- Preços muito baixos comparados ao normal.
- Apenas pagamentos por PIX ou cartão à vista.
- Mensagens urgentes: ”Última channce!”, ”Só até hoje!”.

**Dica: Nunca compre com pressa. Duvide de ofertas milagrosas.**

## 2.6. Como saber se um site de compras é confiável

- Tem o símbolo de cadeado na barra de pesquisa e o link começa com https:// ?
- Procure o CNPJ, o endereço físico e alguma forma de contato da loja.
- Pesquise o nome da loja com as palavras ”é confiável?” ou ”tem reclamações?”

**Ferramentas para verificar**

- www.consumidor.gov.br - Reclamações de consumidores.
- www.reclameaqui.com.br - opiniões sobre lojas.
- Consulte o CNPJ da loja para saber se a empresa existe mesmo.

## 2.7. Golpes comuns e como se proteger

### 2.7.1 Golpe do PIX/ WhatsApp clonado:

Nesse golpe, a pessoa finge ser um parente/conhecido e pede dinheiro. Uma forma de se proteger é ligar para a pessoa que o golpista está se passando, confimando se ela pediu o dinheiro ou se o seu WhatsApp foi clonado.

Caso a pessoa com WhatsApp clonado seja você, avise seus contatos e ative a verificação em duas etapas (por exemplo, um código de segurança para acessar o WhatsApp).

### 2.7.2 Promoção falsa:

Em algum site ou até mesmo por meio de SMS, aparecerá a mensagem "Você ganhou um prêmio! Clique aqui para receber!". Não clique, pois há chances enormes de ser golpe. Apenas apague a mensagem ou saia do site e não compartilhe o link ou a mensagem.

### 2.7.3 Golpe do banco:

Entram em contato (seja por meio de mensagem via SMS ou WhatsApp, ou por meio de ligação) dizendo que sua conta foi bloqueada. Caso isso aconteça, desligue a ligação ou não responda a mensagem, também não clique em links que tenham sido disponibilizados. Importante destacar que bancos não pedem senha por mensagem, para confirmar se não nenhum erro ou atividade suspeita na sua conta, ligue diretamente para o número oficial e seguro do banco ou entre no aplicativo oficial e confirme as informações.

**Pare, pense e verifique!**

### 2.7.4 Antes de comprar ou clicar:

1. Desconfie de promoções muito boas
2. Verifique o site, CNPJ da loja e se tem reclamções
3. Não compartilhe senhas ou dados bancários e nem envie dinheiro sem ter certeza.
4. Se parecer estranho, provavelmente é golpe!

# 3. Contas bancárias digitais

## 3.1. Como acessar sua conta bancária digitial?

O primeiro passo para acessar sua conta bancária por um aplicativo de celular é instalar o aplicativo no seu aparelho celular. Para isso, entre na Play Store e pesquise o nome do banco desejado. Neste processo, é importante verificar se o aplicativo que está sendo baixado é realmente o aplicativo oficial do banco, confirmando sua avaliação e alguns comentários deixados na aba do aplicativo.

Após a instalação do aplicativo, está na hora de, efetivamente, acessar a sua conta pelo aplicativo. Importante ressaltar que cada banco utiliza um sistema de segurança diferente, portanto, pode ser que haja uma diferença no processo de acesso a depender do banco que será acessado

### 3.1.1 Banco itaú

Após abrir o aplicativo, aparecerá as opções ''Acessar" e ''Não sou cliente". Clique em ''Acessar". Após isso, é digitar sua agência e conta e clicar no continuar presente no inferior da tela. Por medidas de segurança, o itaú também pede, após isso, que você digite a senha do seu internet baking, que é uma senha diferente da senha utilizada nos cartões.

Caso não queira entrar pelos dados de agência e conta, após clicar em ''Acessar", ao abrir o aplicativo, clique em ''Entrar com CPF" presente no canto inferior esquerdo. Após isso, utilize a sua senha do internet baking.

### 3.1.2 Banco Bradesco

Após abrir o aplicativo, já aparecerá para colocar agência e conta. Logo embaixo de onde coloca esses dados, terá as opções de ''1º titular"; ''2º titular" e ''3º titular". É fundamental selecionar uma dessas opções para que consiga entrar na conta. Clique em entrar, após preencher todos os dados, e coloque a senha de acesso a conta. Por último, clique em continuar no inferior da tela

### 3.1.3 Banco Santander

Após abrir o aplicativo, clique em entrar. Embaixo de ''Digite seu CPF" terá uma ''caixa" em branco. Clique na caixa em branco e digite seu CPF, clique em continuar no inferior da tela. Após isso, embaixo de Digite a senha de acesso, digite sua senha e clique em ''Entrar no inferior da tela". Após entrar, o banco pedirá algumas permissões básicas para envio de notificações e gerenciamento de chamadas, que podem ser permitidas.

### 3.1.4 Banco Nubank

Após abrir o aplicativo, clique em começar no inferior da tela. Digite o seu CPF no campo em branco já com o exemplo de CPF preenchido com vários 0's. Após isso, digite sua senha, que não é a senha do banco, mas a senha que você cadastrou para entrar no aplicativo.

## 3.2. Salvamento dos dados bancários

Para maior segurança dos seus dados bancários e para que eles não caiam em mãos de pessoas mal-intencionadas, são necessários alguns cuidados por parte do usuário.

1. Uso de senhas fortes que mesclem, quando possível, números, letras maiúsculas e minúsculas e símbolos.

2. Cuidado com a rede de internet que está sendo utilizada quando estiver acessando o aplicativo do banco. (Algumas redes públicas ou desconhecidas podem, ao ser conectadas, acessar os dados sensíveis do usuário - como senha e número de agência – que podem ser utilizadas de forma maliciosa. Dê preferência a redes de internet já conhecidas e de confiança).

3. Nunca clique em links de SMS de origem desconhecida. Mesmo que a mensagem diga ser do banco, desconfie. Quanto mais urgente ou quanto melhor a oferta feita pelo SMS parece, mais provável de ser golpe.

4. Para além da senha de acesso, se possível, ative outros fatores de autenticação (como a impressão digital ou biometria facial).

5. Utilize o cartão virtual. Atualmente, a maioria dos bancos oferecem o serviço do cartão virtual. O cartão virtual pode ser feito na hora, e excluído a qualquer momento, sendo, dessa forma, mais seguro.

6. Não anote suas senhas ou dados pessoais no celular. Se possível, faça senhas intuitivas que possam ser lembradas quando necessário. Caso não seja possível, anote em um caderno que ficará apenas em casa, já que há a possibilidade de também roubarem o caderno ou papel com estes dados caso sejam levados na bolsa ou mochila.

7. Sempre mantenha o sistema do seu celular atualizado. Essas atualizações são feitas justamente para corrigir possíveis problemas de segurança que possam estar presente no sistema antigo. Por isso, é importante atualizar tanto o sistema do celular quanto o aplicativo do banco.

8. Nunca compartilhe os dados do cartão por meio de Whatsapp ou redes sociais, elas podem ser hackeadas e pessoas mal-intencionadas podem ter acesso a esses dados.

## 3.3. Medidas de segurança em caso de assalto ou perda do aparelho celular

O primeiro passo a se fazer em caso de assalto ou perda do aparelho celular é ligar para o atendimento do banco com o objetivo de notificar o banco responsável pela sua conta do ocorrido, para que assim a instituição inicie o processo de bloquear o cartão e o acesso ao aplicativo do banco por outros aparelhos celular.

Caso queira bloquear o acesso ao celular, é importante fazer o boletim de ocorrência. Após isso, ligue na operadora e informe o IMEI do aparelho celular (O MEI está presente tanto na caixa do aparelho quanto na nota fiscal). Abaixo segue uma tabela com os números para contato das principais instituições financeiras.

| Instituição Bancária | Número para atendimento |
|---|---|
| Nubank | 4020 0185 ou 0800 608 6236 |
| Itáu | 4004 4828 ou 0800 970 4828 |
| Santander | 4004 3535 ou 0800 702 3535 |
| Bradesco | 4002 0022 ou 0800 570 0022 |
| Caixa | 4004 0104 ou 0800 104 0104 |

# 4. Praticando

### 4.0.1 Atividade - senhas fortes

- Leia com atenção cada pergunta e marque a alternativa correta
- Marque apenas uma alternativa em cada pergunta

1. **O que é uma senha forte?:**

   (a) ( ) Uma senha como 123456 ou meu nome.
   (b) ( ) Uma senha que tem letras, números e símbolos.
   (c) ( ) Minha data de nascimento.

2. **Qual dessas senhas é uma senha segura?**

   (a) ( ) Maria2024
   (b) ( ) 123456
   (c) ( ) 334455Mct3j&1p!

3. **Onde é mais seguro guardar sua senha?**

   (a) ( ) Em um papel jogado na mesa.
   (b) ( ) Numa foto dentro do celular.
   (c) ( ) Num caderno guardado em um lugar seguro na sua casa.

4. **Por que não é seguro deixar sua senha salva no celular, no computador ou no Google?**

   (a) ( ) Porque qualquer pessoa que pegar meu celular ou computador
   (b) ( ) Porque assim eu nunca mais esqueço a senha
   (c) ( ) Por que o celular protefe sozinha e não deixa ninguém ver.

5. **Quando é recomendado trocar sua senha?**

   (a) ( ) Nunca precisa trocar.
   (b) ( ) Só quando esquecer.
   (c) ( ) Se perceber algo estranho ou a cada 3 meses

6. **Qual dessas situações é um sinal de golpe na internet?**

   (a) ( ) Receber mensagem pedindo minha senha ou meus dados bancários para confirmar cadastro, vaga de emprego ou prêmio.
   (b) ( ) Receber uma mensagem do meu irmão perguntando meu endereço
   (c) ( ) Alguém me pedir meu número de telefone para me ligar

7. **O que é um símbolo usado na senha?**

   (a) ( ) Uma letra, como, por exemplo, a letra A.

   (b) ( ) Um número, como, por exemplo, o número 7.

   (c) ( ) Um sinal ou símbolo, como, por exemplo, os símbolos @, , & e !

### 4.0.2 Atividade sobre Fake News

1. **Leia com atenção as duas notícias a seguir e responda à questão proposta.**

   **Notícia 1**

   **"Beber água gelada faz o pulmão congelar e pode levar à morte"**

   Uma mensagem que circula em grupos de WhatsApp diz que beber água gelada, especialmente no inverno, pode causar o congelamento dos pulmões e até levar à morte. O texto alerta as pessoas a só beberem água morna ou em temperatura ambiente.

   **Notícia 2**

   **Governo amplia acesso a especialistas no SUS com novo programa de Saúde Publica**

   O Ministério da Saúde anunciou, em junho de 2025, a ampliação do programa "Agora Tem Especialistas", com o objetivo de reduzir a fila de espera por consultas, exames e cirurgias especializadas no Sistema Único de Saúde (SUS). A medida vai beneficiar pacientes que aguardam atendimentos em áreas como cardiologia, ortopedia, oftalmologia, oncologia e saúde da mulher.

   **Agora é com você:**

   (a) Qual notícia é Fake News?

   (b) Qual notícia é verdadeira?

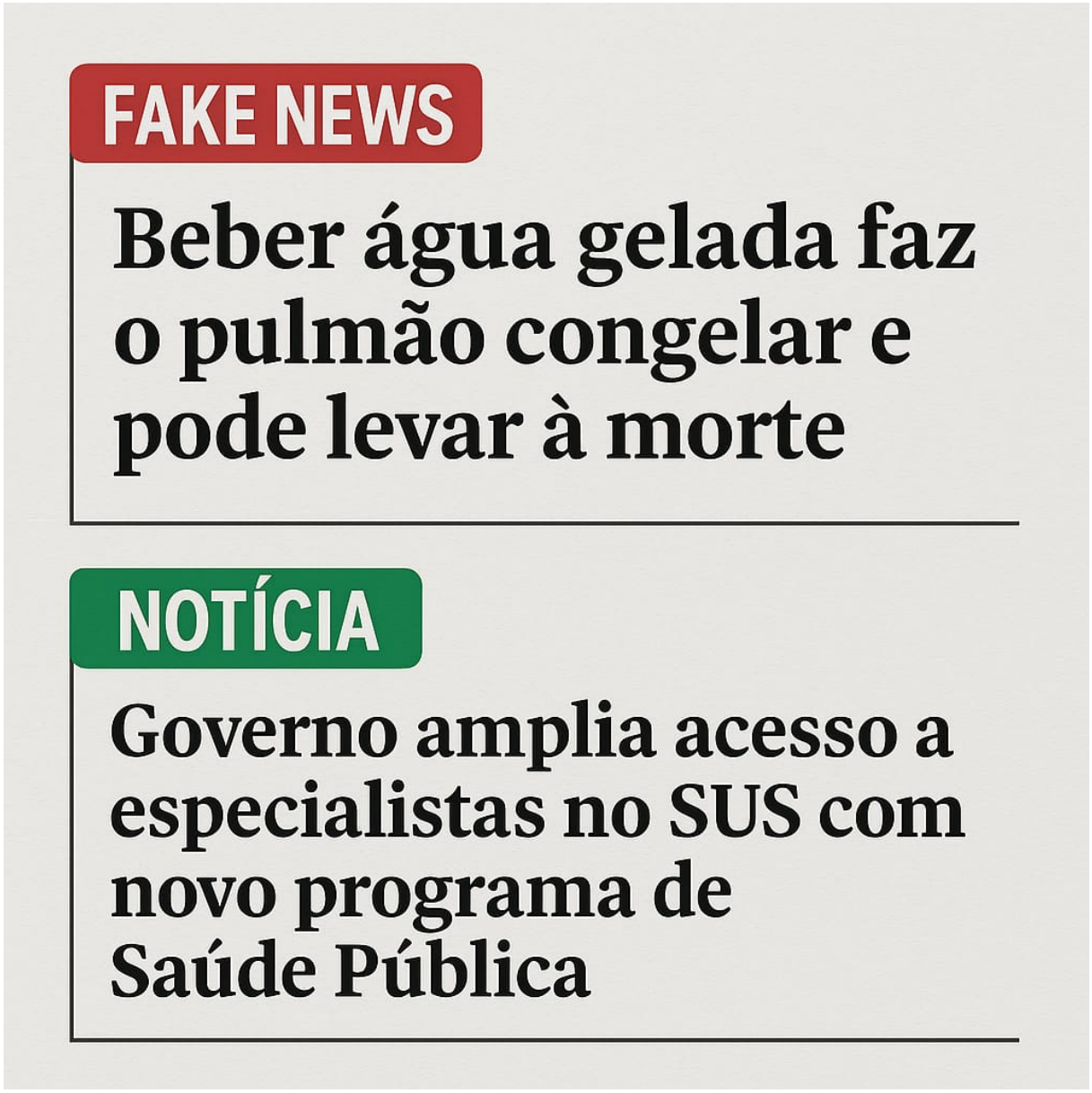
   (c) Como você chegou a essa conclusão?

   **Resolução**

   Após a leitura das duas notícias, vamos analisar, então, quais características evidenciam que a notícia 1 é a Fake News.

   **Por que a notícia 1 é fake news?**

   Os pulmões ficam protegidos dentro do corpo, e a temperatura interna não permite que isso aconteça. Não há nenhum caso médico comprovado sobre esse risco.




**Por que a notícia 2 é verdadeira?**

A notícia foi divulgada nos principais sites oficiais de saúde através da fonte oficial, sendo ela: Ministério da Saúde – Programa Agora Tem Especialistas: https://www.gov.br/saude/p br

**Vamos desmembrar:**

Qual a origem da notícia?

Enquanto a primeira notícia é espalhada pelo WhatsApp, onde não se sabe de onde veio sua origem, a segunda notícia foi retirada de um site confiável, como o do Ministério da Saúde. Saber a origem da notícia que se está lendo é um ótimo começo para se desconfiar que se trata de uma Fake News.

Qual a origem dos dados relatados na notícia?

Enquanto a primeira notícia não deixa claro a origem dos dados (fonte onde foi tirada), a segunda notícia deixa claro que os dados são retirados de dados retirados do Ministério da Saúde.

#### 4.0.3 Atividades sobre acesso à apps bancários e segurança dos dados bancários

1. **Com as palavras dispostas abaixo, complete as frases de forma correta**

   | senha | aplicativo | internet | cartão virtual | CPF |

   (a) Para acessar sua conta digital, o primeiro passo é instalar o _____ oficial do banco.

   (b) Nunca clique em links suspeitos que chegam por mensagem de texto ou _____.

   (c) Nunca anote sua _____ no celular ou envie por redes sociais.

   (d) Uma forma mais segura de fazer compras online é usando o _____ .

   (e) Alguns bancos permitem o acesso à conta apenas com o número do _____.

2. **Leia as frases marque (V) para verdadeiro ou (F) para falso:**

| FRASE | VERDADEIRO | FALSO |
|---|---|---|
| Todas as senhas devem ser iguais: pode-se usar a mesma para tudo | ____ | ____ |
| É importante manter o celular sempre atualizado. | ____ | ____ |
| Se você perder o celular, deve avisar o banco o mais rápido possível | ____ | ____ |
| Redes públicas de Wi-fi são recomendadas para acessar sua conta bancária | ____ | ____ |
| Cartão virtual pode ser excluído a qualquer momento | ____ | ____ |

# 5. Conclusão

A internet é uma ótima forma de fazer as coisas do nosso cotidiano com mais praticidade e conforto, sendo uma ferramenta necessária nos dias atuais. Mas, para conseguir utilizar a internet com segurança e eficiência, é preciso ter atenção e estar sempre atento.

# 6. Materiais Complementares

- Vídeo: https://www.youtube.com/watch?v=8uZN5U06s6o
- Vídeo: https://www.youtube.com/watch?v=LX48gDGblxQ
- Vídeo: https://www.youtube.com/watch?v=DZXmpbr13a0

# 7. Referências do Módulo


Bradesco. (n.d.). *Dicas de segurança: prevenção de golpes.* Acesso em 12 de junho de 2025. https://banco.bradesco/seguranca/prevencao-de-golpes/dicas-de-seguranca.shtm

Caixa Econômica Federal. (n.d.). *Cartões Caixa: segurança.* Acesso em 12 de junho de 2025. https://www.caixa.gov.br/seguranca/cartoes-caixa/Paginas/default.aspx

Itaú. (n.d.). *Sofreu roubo, furto, perda ou golpe? Saiba como se proteger.* Acesso em 12 de junho de 2025. https://shre.ink/eU88

Itaú. (2024, maio). *Segurança digital: entenda o que é e 5 dicas para se proteger.* Blog Itaú. Acesso em 12 de junho de 2025. https://encurtador.com.br/2wiMd

Neves, M. (2023, 11 de março; atualizado em 18 de janeiro de 2025). *Segurança digital: tudo que você precisa saber.* Fala, Nubank. Acesso em 12 de junho de 2025. https://blog.nubank.com.br/seguranca-digital-tudo-que-voce-precisa-saber/

Nubank. (2020, 5 de março; atualizado em 4 de outubro de 2024). *Teve o celular roubado? Saiba o que fazer.* Fala, Nubank. Acesso em 12 de junho de 2025. https://blog.nubank.com.br/celular-roubado-o-que-fazer/

Santander. (2025, 30 de maio). *Foi furtado ou roubado? Entenda o que fazer em seguida. Blog Santander.* Acesso em 12 de junho de 2025.https://encurtador.com.br/93arS

Santander. (2024, 28 de outubro). *Segurança Digital no Santander: Como manter se seguro de forma online.* Blog Santander. Acesso em 12 de junho de 2025. https://www.santander.com.br/blog/seguranca-digital-santander