FORMAÇÃO
SAÚDE
DIGITAL
NO SUS

Passo a passo para manter-se seguro on-line

Apresentação

O uso crescente de recursos digitais no dia a dia — da comunicação ao estudo, do trabalho ao entretenimento — nos mostra a importância de práticas voltadas à segurança no ambiente virtual. Com a popularização da internet e a constante troca de informações on-line, surgem também diferentes tipos de riscos, como acessos não autorizados, vazamento de dados e tentativas de fraude.

Diante desse cenário, entender como utilizar os meios digitais de forma segura tornou-se essencial para usuários com diferentes perfis. Isso envolve não apenas o uso de ferramentas adequadas, mas também a adoção de comportamentos preventivos. Medidas como criar senhas seguras, verificar a confiabilidade de links e proteger informações pessoais são exemplos práticos de como reduzir a exposição a riscos virtuais.

Ao adotarmos comportamentos conscientes e preventivos, é possível navegar na internet com mais segurança, proteger nossas informações e evitar transtornos. Estar seguro no ambiente digital não é mais uma opção, mas sim uma necessidade constante em nosso cotidiano.

OBJETIVO DE APRENDIZAGEM

A partir deste material, você irá reconhecer estratégias para o uso seguro de recursos digitais.

Passo a passo para manter-se seguro on-line

*Você conhece as plataformas: **Facebook**, **Instagram**, **X** e **Tik Tok**? Talvez já tenha ouvido falar ou utilize alguma delas, certo? Você conhece esses aplicativos de mensagens: **Whatsapp** e **Telegram**? E uma última pergunta, não menos importante, você sabe quantas informações você compartilha na internet?*

Os brasileiros passam, em média, mais de três horas por dia nas redes sociais, tornando o Brasil um dos países que mais utilizam redes sociais no mundo[1].

Essa presença digital mudou a forma como nos comunicamos, buscamos informações e até como empresas e governos se relacionam com as pessoas.

Hoje, as redes sociais são usadas para diversas finalidades, como publicidade, educação e até campanhas políticas, permitindo que muitas informações circulem rapidamente e alcancem milhões de pessoas em poucos segundos. Infelizmente, nem tudo são vantagens. O uso intenso dessas plataformas também traz riscos[2].

Muitas pessoas mal-intencionadas aproveitam a confiança dos usuários para aplicar golpes e roubar informações pessoais. Isso pode acontecer de várias formas:

Mensagens falsas que pedem senhas;

Links suspeitos que instalam vírus;

Ou até perfis falsos que se passam por conhecidos para enganar as vítimas.

Esses ataques podem causar problemas sérios, como perdas financeiras, roubo de dados pessoais e exposição de dados privados.

Você já recebeu ou soube de alguém que tenha recebido mensagens parecidas com essa em aplicativos de mensagens?

Este é um golpe bastante comum, no qual estelionatários se passam por um familiar ou conhecido para pedir transferências bancárias. Mas este não é o único perigo que corremos quando estamos on-line.

Fonte: Adaptado de Canva.com

Organizamos a seguir alguns golpes[2] para que você conheça e não caia nessa!

SIM SWAP – "Golpe do número telefônico chip"

- *SIM SWAP* – Esse termo vem do inglês, que significa troca do SIM. Ataque em que criminosos transferem o número de telefone de uma vítima para outro chip SIM, para obter acesso a contas protegidas por SMS.

Os criminosos roubam seu número de telefone e transferem para outro chip. Com isso, eles conseguem receber mensagens e códigos de segurança enviados por SMS, podendo invadir suas contas bancárias, redes sociais e outros serviços. Isso pode causar grandes prejuízos, como roubo de dinheiro e vazamento de informações pessoais.

O que fazer para se proteger?

- Evite compartilhar seus dados;
- Ative a verificação em duas etapas;
- Se perceber que seu celular parou de funcionar sem motivo, entre em contato com a operadora imediatamente.

Golpe do falso suporte técnico

- Esse golpe acontece quando uma pessoa está usando redes sociais e recebe uma mensagem ou anúncio dizendo que seu celular ou computador tem um problema, como vírus ou falha de segurança. A mensagem parece vir de uma empresa de tecnologia ou de suporte técnico confiável, pedindo que a pessoa clique em um link ou ligue para um número de telefone para resolver o problema.

Se a pessoa clicar no link, será levada para um site falso que parece real, mas que, na verdade, é controlado por golpistas. Eles podem pedir informações pessoais, senhas ou até mesmo cobrar por um serviço que não existe.

O que fazer para se proteger?

- Nunca clique em links suspeitos;
- Se precisar de suporte técnico, procure diretamente os canais oficiais da empresa.

Golpe dos perfis falsos

- Os golpistas aplicam esse golpe acessando contas de redes sociais de outras pessoas ou criando perfis falsos com o nome e as fotos da vítima. Depois que conseguem uma conta ou criam um perfil convincente, começam a mandar mensagens para amigos e familiares fingindo ser a pessoa verdadeira.

Nas mensagens, os golpistas costumam dizer que estão passando por uma emergência, como um roubo, um acidente ou um problema de saúde, e pedem dinheiro com urgência. Outra tática comum é fingir que perderam o acesso à conta original e que criaram um novo perfil, entrando em contato com amigos para "avisar".

O que fazer para se proteger?

- Sempre confirme com a pessoa por ligação ou vídeo antes de enviar qualquer dinheiro.

Golpe de loteria ou prêmio falso

- Esse golpe acontece quando a pessoa recebe uma mensagem ou vê um anúncio em redes sociais, como Facebook, Instagram ou WhatsApp, dizendo que ganhou um prêmio, um sorteio ou até uma loteria. Os golpistas fingem ser representantes de empresas conhecidas ou até usam contas falsas de amigos para parecer mais convincentes.

As mensagens costumam ser bem-feitas, usando imagens, logotipos e textos que fazem tudo parecer real. Elas dizem que a pessoa ganhou dinheiro, um carro ou uma viagem, mas, na verdade, é um golpe. Normalmente, os criminosos pedem que a vítima pague uma "taxa" ou forneça dados pessoais para receber o prêmio.

O que fazer para se proteger?

- Se você não participou de nenhum sorteio, não pode ter ganhado nada;
- Nunca passe seus dados ou faça pagamentos sem ter certeza de que a promoção é verdadeira.

Conhecer esses golpes é uma forma de prevenir os sérios problemas que eles podem trazer. Por isso, é fundamental estarmos atentos às informações que compartilhamos e sempre verificar o que estamos recebendo. Proteger seus dados e evitar cair em golpes é uma forma de garantir mais segurança para você e sua família.

Quer saber como? Vamos fortalecer a sua segurança com boas práticas.

Dicas para segurança on-line

Para proteger suas informações na internet, como se fossem seus documentos pessoais, siga estas dicas[3]:

1. **Crie senhas fortes e diferentes** para cada site ou aplicativo que você usa. Não use informações fáceis de descobrir, como nomes de parentes ou datas de nascimento. Se precisar de ajuda para criar e guardar senhas complicadas, use um gerenciador de senhas.

2. **Ative a autenticação em duas etapas** sempre que possível. Isso significa que, além da senha, você precisará de um código extra para acessar suas contas, como um código enviado para o seu celular.

3. **Mantenha seus aparelhos, como celular e computador, sempre atualizados** com os programas de segurança mais recentes. Isso ajuda a evitar que pessoas más usem falhas de segurança para invadir seus dispositivos.

4. **Tenha cuidado com *links*** e mensagens estranhas que você recebe por e-mail, WhatsApp ou redes sociais. Não clique em links suspeitos e nunca forneça seus dados pessoais ou bancários por e-mail ou mensagens de pessoas que você não conhece.

5. **Use redes de internet seguras**, como a da sua casa, principalmente para acessar sites de bancos ou fazer compras on-line. Evite usar redes wi-fi públicas para essas atividades.

6 **Verifique sempre as configurações de privacidade** dos seus aplicativos e redes sociais. Limite a quantidade de informações pessoais que você compartilha e escolha quem pode ver suas publicações.

7 **Evite compartilhar informações pessoais importantes**, como números de documentos, telefone ou endereço, em sites ou aplicativos que você não confia.

8 **Use programas de antivírus e outras ferramentas de segurança** nos seus dispositivos para se proteger de vírus e outros perigos da internet.

Outra dica para se proteger de perigos nas redes sociais é saber identificar conteúdos maliciosos. A maioria desses conteúdos tenta levar você para fora da rede social ou obter suas informações pessoais para usá-las de forma indevida. Fique atento a links suspeitos e use ferramentas on-line, como o "SiteConfiável", para verificar se um site é seguro antes de acessá-lo.

Desconfie de sites com erros de digitação, *design* ruim ou ofertas muito vantajosas.

Verifique sempre se o endereço do site é o correto, sem erros ou variações estranhas.

Tenha cuidado com mensagens que criam um senso de urgência, como aquelas que pedem dinheiro ou informações pessoais de forma repentina.

Procure confirmar essas mensagens com amigos e familiares por outros meios de comunicação.

Lembre-se:
A prevenção é a melhor forma de se proteger de golpes e fraudes on-line.

Referências

1. MELTWATER. **2024 global digital report**. Disponível em: https://www.meltwater.com/en/2024-global-digital-trends. Acesso em: 22 abr. 2025.

2. SANTOS, D. E. G. **Segurança digital em redes sociais**. 1. ed. Santa Maria, RS: UFSM, CTE, 2024.

3. COSTA, P. R. M. B.; SOUSA, P. L. V.; DA SILVA, T. M. **Proteção dos dados pessoais no ambiente digital**. Centro Universitário UniProcessus, 2024. Disponível em: https://spgaex.processus.edu.br/wp-content/uploads/2024/07/2-DESENVOLVIMENTO-1.pdf. Acesso em: 22 abr. 2025.

Créditos

Secretaria de Informação e Saúde Digital - SEIDIGI
Ana Estela Haddad

Coordenação do Projeto
Paola Trindade Garcia

Coordenação-Geral da UNA-SUS/UFMA
Elza Bernardes Ferreira

Vice-Coordenação da UNA-SUS/UFMA
Ana Emilia Figueiredo de Oliveira

Elaboração dos conteúdos
Isabelle Aguiar Prado

Recursos Educacionais

Helen Maysa Belfort Sousa
Letícia Iane de Holanda Ribeiro
Designers Instrucionais

Jackeline Mendes Pereira
Priscila Penha Coelho
Designers Gráficas

Mizraim Mesquita Nunes
Talita Guimarães Santos Sousa
Revisoras Textuais

Interface Gráfica
Geovana Soares Silveira
Jackeline Mendes Pereira

Tecnologia da Informação
Osvaldo Silva de Sousa Junior
Coordenador

Heber de Padua Sousa
Desenvolvedor Mobile

Arthur Marinho dos Passos
Desenvolvedor Mobile

Antonio Marcos Vieira Sales
Desenvolvedor full stack

COMO CITAR ESTE MATERIAL

PRADO, Isabelle Aguiar. **Passo a passo para manter-se seguro on-line**. São Luís, MA: UFMA; SEIDIGI/MS, 2025. 10 p. Material digital elaborado para compor o acervo da Biblioteca Digital da SEIDIGI/MS.