SEGURANÇA DIGITAL

PARA TODOS

Guia prático para proteger você e sua família no mundo digital

Projeto de Extensão
Universidade Paulista - UNIP
Bacharelado em Ciência da Computação

Aluno: Wilian Damasio
Mogi Mirim - SP | 2026

ODS 9 - Indústria, Inovação e Infraestrutura

APRESENTAÇÃO

Você já parou para pensar quantas vezes por dia usa seu celular para acessar o banco, fazer compras, conversar com amigos ou consultar informações? A tecnologia facilita nossa vida, mas também traz riscos que muitas pessoas desconhecem.

Esta cartilha foi criada para ajudar você, sua família e sua comunidade a navegar com mais segurança no mundo digital. Aqui você vai encontrar dicas práticas, explicadas de forma simples, para proteger seus dados, evitar golpes é usar a internet de forma mais consciente.

O conteúdo foi desenvolvido como parte do Projeto de Extensão do curso de Bacharelado em Ciência da Computação da Universidade Paulista (UNIP), com o objetivo de levar conhecimento tecnológico acessível para a comunidade local.

Não importa sua idade ou nível de familiaridade com tecnologia: esta cartilha é para você. Leia, compartilhe e coloque as dicas em prática. Juntos, podemos construir uma comunidade digital mais segura.

> **Boa leitura! Compartilhe este material com familiares e amigos.**

SUMÁRIO

1. O que é segurança digital e por que importa
2. Senhas seguras: como criar e gerenciar
3. Golpes comuns: Pix, WhatsApp, links falsos, boletos
4. Como proteger seu celular
5. Backup: o que é e como fazer
6. Privacidade nas redes sociais
7. Wi-Fi seguro em casa e no trabalho
8. O que fazer se cair em um golpe
9. Recursos e contatos úteis
10. Sobre o projeto e créditos

1. O QUE É SEGURANÇA DIGITAL E POR QUE IMPORTA

Segurança digital é o conjunto de práticas e cuidados que tomamos para proteger nossos dados, nossa privacidade e nossos dispositivos (celular, computador, tablet) contra ameaças na internet.

Assim como trancamos a porta de casa e tomamos cuidado com nossos documentos físicos, precisamos ter o mesmo cuidado com nossas informações no mundo digital. Senhas, fotos, dados bancários, conversas pessoais: tudo isso pode ser acessado por pessoas mal-intencionadas se não tomarmos as precauções adequadas.

Por que você deve se preocupar?

- O Brasil é um dos países com mais vítimas de golpes digitais no mundo
- Em 2023, mais de 80 mil pessoas foram vítimas de golpes via Pix, segundo o Banco Central
- Celulares roubados ou perdidos podem expor toda sua vida digital: banco, e-mail, redes sociais
- Idosos e pessoas com menos familiaridade digital são os alvos mais frequentes

A boa notícia é que a maioria dos golpes pode ser evitada com conhecimento e alguns cuidados simples, que você vai aprender nas próximas páginas.

> **A melhor proteção e a informação. Quanto mais você sabe, mais difícil e ser enganado.**

2. SENHAS SEGURAS: COMO CRIAR E GERENCIAR

Sua senha é a chave da sua vida digital. Se alguém descobre sua senha, pode acessar seu e-mail, banco, redes sociais e muito mais. Por isso, criar senhas fortes é o primeiro passo para se proteger.

O que é uma senha forte?

Uma senha forte tem pelo menos 8 caracteres e mistura diferentes tipos de caracteres:

- Letras maiúsculas (A, B, C...)
- Letras minúsculas (a, b, c...)
- Números (0, 1, 2, 3...)
- Símbolos (@, #, $, !, ?...)

SENHAS QUE VOCÊ NUNCA DEVE USAR
123456, 123456789, senha, password
Seu nome, nome do filho, nome do pet
Data de nascimento (sua ou de familiares)
Número de telefone
Qualquer palavra do dicionario sozinha

Dica: crie senhas com frases

Pense numa frase que só você conhece e transforme em senha:

Exemplo: Meu cachorro Rex tem 5 anos!

Senha: McRt5a! (primeiras letras de cada palavra + números + símbolo)

Essa técnica cria senhas fáceis de lembrar e difíceis de adivinhar.

Uma senha para cada conta

Nunca use a mesma senha em sites diferentes. Se um site for invadido e sua senha vazar, o criminoso vai tentar essa mesma senha no seu e-mail, banco e redes sociais.

DICA: GERENCIADORES DE SENHAS
Use um app gerenciador de senhas para guardar todas as suas senhas com segurança.
Opções gratuitas: Google Password Manager (integrado ao Chrome/Android), Bitwarden.
Você só precisa lembrar de UMA senha mestra. O app cuida do resto.

Verificação em duas etapas

Ative a verificação em duas etapas (2FA) em todas as contas que oferecem essa opção. Com ela, além da senha, você precisa confirmar o acesso com um código enviado ao seu celular. Mesmo que alguém descubra sua senha, não conseguirá entrar sem o código.

Como ativar: procure nas Configurações > Segurança da sua conta (Google, Facebook, Instagram, banco, etc.).

3. GOLPES COMUNS: PIX, WHATSAPP, LINKS FALSOS

Conhecer os golpes mais comuns é a melhor forma de evitá-los. A seguir, os principais golpes que atingem a população brasileira:

Golpe do WhatsApp clonado

O criminoso se passa por um amigo ou familiar e pede dinheiro urgente via Pix. Ele pode ter clonado o número da pessoa ou criado uma conta falsa com a foto dela.

> **REGRA DE OURO: recebeu pedido de dinheiro pelo WhatsApp? LIGUE para a pessoa antes de transferir.**

- Desconfie de urgência excessiva (preciso agora, e emergência)
- Verifique se o número e realmente da pessoa
- Se a pessoa só responde por texto e não atende ligação, é golpe

Golpe do Pix falso

O golpista mostra um comprovante falso de Pix para convencer você de que o pagamento foi feito. O comprovante parece real, mas o dinheiro nunca entrou na conta.

- Sempre confira no app do banco se o valor realmente caiu
- Nunca confie apenas em prints de comprovante
- Espere o dinheiro cair antes de entregar o produto ou serviço

Phishing: links e e-mails falsos

Você recebe um SMS, e-mail ou mensagem no WhatsApp dizendo que seu cartão foi bloqueado, que você ganhou um prêmio ou que precisa atualizar seus dados. O link leva a um site falso idêntico ao do banco ou loja.

SINAIS DE GOLPE POR LINK
Mensagem com urgência: Seu cartão será bloqueado em 24h!
Link com endereço estranho: banc0-segurança.xyz em vez de banco.com.br
Pede dados pessoais: CPF, senha, número do cartão
Erros de português no texto
Remetente desconhecido ou número curto

> **LEMBRE-SE: bancos NUNCA pedem senha, número do cartão ou código de segurança por e-mail, SMS ou WhatsApp.**

Golpe do boleto falso

O golpista envia um boleto falso por e-mail ou WhatsApp, com aparência idêntica ao real, mas com o código de barras alterado para direcionar o pagamento para a conta dele.

- Sempre confira os dados do beneficiário antes de pagar (nome, CNPJ)
- Prefira gerar boletos diretamente no site ou app oficial da empresa
- Desconfie de boletos recebidos por e-mail sem ter solicitado

4. COMO PROTEGER SEU CELULAR

Seu celular contém praticamente toda a sua vida digital: banco, e-mail, fotos, conversas, documentos. Protege-lo é fundamental.

Bloqueio de tela

- Ative o bloqueio por senha, PIN ou biometria (digital/reconhecimento facial)
- Nunca deixe o celular sem bloqueio de tela
- Evite padrões de desbloqueio simples (L, Z, quadrado)

Atualizações do sistema

- Mantenha o Android ou iOS sempre atualizado
- As atualizações corrigem falhas de segurança que criminosos podem explorar
- Ative as atualizações automáticas: Configurações > Sistema > Atualização

Aplicativos seguros

- Instale apps apneas da Play Store (Android), ou App Store (iPhone)
- Verifique as avaliações e o desenvolvedor antes de instalar
- Desinstale apps que você não usa mais
- Revise as permissões dos apps: câmera, microfone, localização

Em caso de roubo ou perda

PASSOS IMEDIATOS SE SEU CELULAR FOR ROUBADO
1. Ligue para o banco e bloqueie o app bancário
2. Bloqueie o chip ligando para a operadora
3. Acesse android.com/find (Android) ou icloud.com/find (iPhone) para localizar ou apagar remotamente
4. Troque as senhas do e-mail, redes sociais e banco por outro dispositivo
5. Registre um B.O. na delegacia (pode ser online)
6. Bloqueie o IMEI ligando para a operadora (o número está na caixa do celular ou em *#06#)

5. BACKUP: O QUE É E COMO FAZER

Backup é uma cópia de segurança dos seus arquivos. Se o celular quebrar, for roubado ou der defeito, você não perde fotos, contatos, documentos e mensagens porque tudo está salvo em outro lugar.

Como ativar o backup no Android

- Configurações > Google > Backup > Ative o Backup do Google One
- Isso salva contatos, apps instalados, configurações e histórico de chamadas
- Para fotos: abra o Google Fotos > Configurações > Backup > Ative

Como ativar o backup no iPhone

- Ajustes > [seu nome] > iCloud > Backup do iCloud > Ative
- Para fotos: Ajustes > [seu nome] > iCloud > Fotos > Ative

Backup de documentos importantes

Além do celular, salve documentos importantes do computador na nuvem:

- Google Drive: 15 GB gratuitos, acesse de qualquer lugar
- OneDrive (Microsoft): 5 GB gratuitos, integrado ao Windows

> **DICA: conecte no Wi-Fi antes de fazer o primeiro backup. Pode ser grande!**

De vez em quando, abra o Google Drive ou iCloud e confirme que seus arquivos estão lá. Melhor prevenir do que chorar.

6. PRIVACIDADE NAS REDES SOCIAIS

Redes sociais são ótimas para se conectar com amigos e família, mas também expõe informações pessoais que podem ser usadas por golpistas.

O que você NÃO deve publicar

NUNCA PUBLIQUE NAS REDES SOCIAIS
Fotos de documentos (RG, CPF, CNH, cartão de crédito)
Localização em tempo real (quando está de férias, a casa fica vazia)
Rotina detalhada (horários de saída e chegada, escola dos filhos)
Dados pessoais (endereço completo, telefone, placa do carro)
Fotos de boletos, extratos ou comprovantes financeiros

Configurações de privacidade

- Instagram: Configurações > Privacidade > Conta privada (só seguidores veem)
- Facebook: Configurações > Privacidade > Quem pode ver suas publicações > Amigos
- WhatsApp: Configurações > Privacidade > Foto do perfil / Visto por último > Meus contatos

Cuidado com desconhecidos

Não aceite solicitações de amizade de pessoas que você não conhece. Perfis falsos são usados para coletar informações pessoais, aplicar golpes românticos ou enviar links maliciosos.

7. WI-FI SEGURO EM CASA E NO TRABALHO

Sua rede Wi-Fi é a porta de entrada para todos os dispositivos conectados na sua casa. Se ela não estiver protegida, qualquer pessoa por perto pode usar sua internet ou até acessar seus dados.

Proteja sua rede doméstica

- Troque a senha padrão do roteador (aquela que vem de fábrica)
- Use uma senha forte com letras, números e símbolos
- Acesse o painel do roteador: digite 192.168.1.1 ou 192.168.0.1 no navegador
- Nas configurações Wi-Fi, escolha segurança WPA2 ou WPA3 (nunca WEP)
- Troque também a senha de administrador do roteador

Wi-Fi público: cuidado redobrado

> **NUNCA acesse banco, faça compras ou digite senhas em Wi-Fi público (shopping, café, aeroporto).**

Redes públicas são abertas e podem ser monitoradas por pessoas mal-intencionadas. Para transações sensíveis, prefira usar seus dados moveis (3G/4G/5G).

8. O QUE FAZER SE CAIR EM UM GOLPE

Se você foi vítima de um golpe digital, mantenha a calma e siga estes passos imediatamente:

PASSO A PASSO APÓS CAIR EM UM GOLPE
1. REGISTRE UM B.O. - Acesse a Delegacia Eletrônica do seu estado (delegaciaeletronica.sp.gov.br em SP) ou vá presencialmente. Guarde prints e comprovantes de tudo.
2. AVISE SEU BANCO - Ligue imediatamente para o SAC. Peca o bloqueio de transações e do cartão se necessário. Para Pix, peca o acionamento do MED (Mecanismo Especial de Devolução).
3. TROQUE SUAS SENHAS - Mude as senhas de e-mail, redes sociais e apps bancários. Ative a verificação em duas etapas em todas as contas.
4. AVISE SEUS CONTATOS - Se seu WhatsApp foi clonado, avise amigos e família por outro meio (ligação, SMS). Poste aviso nas redes sociais.
5. DENUNCIE - Denuncie perfis falsos nas plataformas. Registre em consumidor.gov.br se envolver empresa. Para crimes na internet, denuncie em denuncie.org.br (SaferNet).

Mecanismo Especial de Devolução (MED) do Pix

Se você fez um Pix para um golpista, o Banco Central criou o MED: você pode solicitar ao seu banco a devolução do valor. O banco analisa o caso e, se confirmado o golpe, bloqueia o valor na conta do recebedor e faz a devolução. Solicite o MED o mais rápido possível, de preferência nas primeiras horas após o golpe.

9. RECURSOS E CONTATOS UTEIS

Salve estes contatos no seu celular. Em caso de golpe ou dúvida, você sabe exatamente para quem ligar:

Serviço	Contato / Link	Para que serve
CERT.br	cartilha.cert.br	Cartilha de Segurança da Internet
SaferNet Brasil	denuncie.org.br	Denúncia de crimes digitais
Procon	consumidor.gov.br	Problemas com empresas
Delegacia Virtual SP	delegaciaeletronica.sp.gov.br	B.O. online
Disque 181	Ligação telefônica	Denúncia anônima
Banco Central	bcb.gov.br	Informações sobre MED/Pix
Google - Encontrar Dispositivo	android.com/find	Localizar celular Android
Apple - Buscar iPhone	icloud.com/find	Localizar iPhone

10. SOBRE O PROJETO

Esta cartilha foi desenvolvida como parte do Projeto de Extensão do curso de Bacharelado em Ciência da Computação da Universidade Paulista (UNIP).

As atividades de extensão da UNIP têm como objetivos a participação da comunidade acadêmica no desenvolvimento econômico, social, tecnológico e cultural de seu entorno, conforme a Resolução CNE/CES n. 7 de 18 de dezembro de 2018.

Objetivo do projeto

Aplicar os conhecimentos de Ciência da Computação em benefício da comunidade local, promovendo inclusão digital, segurança da informação e digitalização de pequenos negócios.

Objetivos de Desenvolvimento Sustentável (ODS)

Este projeto está vinculado ao ODS 9 - Indústria, Inovação e Infraestrutura, contribuindo para a construção de infraestrutura digital acessível e a promoção da inovação tecnológica na comunidade.

Créditos

Aluno: Wilian

Curso: Bacharelado em Ciência da Computação

Instituição: Universidade Paulista - UNIP

Região: São João da Boa Vista / Mogi Mirim - SP

Parceiro: Pet Shop (Banho e Tosa) - instituição parceira para distribuição

Ano: 2026

Fontes e referências

- CERT.br - Cartilha de Segurança para Internet (cartilha.cert.br)
- SaferNet Brasil (safernet.org.br)
- Banco Central do Brasil - Informações sobre Pix é MED (bcb.gov.br)
- Google Safety Center (safety.google)
- ONU Brasil - Objetivos de Desenvolvimento Sustentável (brasil.un.org/pt-br/sdgs)

Compartilhe esta cartilha com amigos e familiares!

Juntos, construímos uma comunidade digital mais segura.