E-BOOK • SEGURANÇA DIGITAL

Segurança digital no dia a dia da Casa Lar

Como reconhecer e evitar golpes de phishing – guia prático para funcionários e voluntários

Casa Lar Nossa Senhora do Carmo
Coqueiros – Florianópolis/SC

Material elaborado como Atividade de Extensão
Curso Superior de Tecnologia em Gestão da Tecnologia da Informação
Universidade Paulista – UNIP

Autor: Thiago Rodrigues Muniz
Setembro de 2026

APRESENTAÇÃO

Para quem é este e-book

Este material foi escrito para as pessoas que fazem a Casa Lar Nossa Senhora do Carmo funcionar todos os dias: coordenação, equipe administrativa, educadoras, cuidadoras e voluntários. Ninguém precisa entender de informática para usá-lo. A proposta é simples: ensinar a **desconfiar na hora certa** e a **agir com calma** quando uma mensagem, ligação ou e-mail parecer estranho.

Golpes digitais não escolhem vítimas pela idade ou pela escolaridade. Eles funcionam porque exploram pressa, cansaço, boa-fé e vontade de ajudar — características muito presentes em quem trabalha cuidando de outras pessoas. Por isso, uma instituição de acolhimento precisa de uma equipe atenta.

> **Como usar este material**
>
> - Leia um capítulo por vez; cada um leva de 5 a 10 minutos.
> - Os quadros **vermelhos** mostram sinais de perigo; os **verdes**, o que fazer; os **laranja**, dicas práticas.
> - No final há um **checklist** para imprimir e um **quiz** para a equipe testar o que aprendeu.

Sumário

CAPÍTULO 1

Por que a Casa Lar precisa se proteger

Pode parecer que golpistas só se interessam por grandes empresas ou por pessoas ricas. Na prática, acontece o contrário: instituições pequenas costumam ter menos proteção e equipes sobrecarregadas, e por isso são alvos fáceis. Uma casa de acolhimento guarda quatro coisas de muito valor:

O que a Casa Lar guarda	Por que isso atrai golpistas
Informações sigilosas das crianças e adolescentes: documentos, relatórios, histórico familiar, comunicações com a Vara da Infância, Ministério Público e Conselho Tutelar	São dados extremamente sensíveis. O vazamento pode expor as acolhidas a riscos reais e causar danos que não têm como ser desfeitos.
Dinheiro: conta bancária, Pix, doações, pagamentos a fornecedores	Golpes de boleto falso, Pix falso e falso doador desviam recursos que fariam falta à instituição.
Contas digitais: e-mail, WhatsApp, redes sociais da instituição	Uma conta invadida pode ser usada para pedir dinheiro a doadores e parceiros em nome da Casa Lar.
Reputação e confiança	A Casa Lar depende da confiança de doadores, voluntários e do poder público. Um incidente abala essa relação.

O que diz a lei

O **Estatuto da Criança e do Adolescente** (Lei 8.069/1990) garante às crianças e adolescentes o direito ao respeito, que inclui a preservação da imagem e da identidade (art. 17). A **Lei Geral de Proteção de Dados – LGPD** (Lei 13.709/2018) exige cuidado especial com dados de crianças e adolescentes, que devem ser tratados sempre no seu melhor interesse (art. 14).

Na prática: **proteger os computadores e celulares da Casa Lar é também proteger as meninas acolhidas.**

A boa notícia é que a maior parte dos golpes pode ser evitada com hábitos simples, que não custam nada. É disso que tratam os próximos capítulos.

CAPÍTULO 2

O que é phishing

Phishing (pronuncia-se “físhing”) vem de *fishing*, “pescar” em inglês. O golpista joga uma **isca** — uma mensagem que parece legítima — e espera que alguém “morda”: clique num link, abra um anexo, informe uma senha, passe um código ou faça um pagamento.

A isca imita alguém em quem confiamos: o banco, os Correios, a Receita Federal, o Tribunal de Justiça, um fornecedor, um doador conhecido, a própria coordenação da Casa Lar ou até um familiar.

Por onde a isca chega

Canal	Nome técnico	Exemplo típico
E-mail	Phishing	“Sua caixa de e-mail será desativada. Clique aqui para confirmar sua senha.”
SMS	Smishing	“Correios: sua encomenda está retida. Pague a taxa de R$ 4,90 no link.”
WhatsApp / Telegram	Golpe por mensageiro	“Oi, troquei de número. Salva esse aqui e me faz um Pix urgente?”
Ligação telefônica	Vishing	“Aqui é da central de segurança do seu banco. Detectamos uma compra suspeita...”
QR Code	Quishing	Cartaz ou boleto com QR Code adulterado que leva a um site falso ou a um Pix para o golpista.
Redes sociais	Perfil falso	Perfil copiando a Casa Lar pedindo doações para uma conta que não é da instituição.

> **A regra de ouro**
>
> Todo golpe de phishing quer que você faça **uma** destas quatro coisas: **clicar**, **informar**, **pagar** ou **instalar**. Sempre que uma mensagem pedir uma delas, pare e confirme por outro caminho antes de agir.

Por que o phishing funciona

O golpista não “hackeia” o computador; ele engana a pessoa. Para isso, usa gatilhos emocionais:

- **Urgência:** “Você tem 30 minutos”, “sua conta será bloqueada hoje”.
- **Medo:** “Há um processo contra a instituição”, “detectamos uma fraude”.
- **Autoridade:** finge ser juiz, delegado, gerente do banco ou a direção.
- **Solidariedade:** “sou um doador e quero ajudar, só preciso dos dados”, “estou em apuros”.
- **Ganância ou curiosidade:** prêmio, reembolso, “veja as fotos”. Se uma mensagem te pressiona, essa sensação já é o primeiro sinal de alerta.

CAPÍTULO 3

Os golpes mais comuns no Brasil

Abaixo estão os golpes que mais atingem instituições e trabalhadores no Brasil, com atenção especial aos que se aproveitam da rotina de uma casa de acolhimento.

Falso boleto ou falsa cobrança de fornecedor

Como funciona: Chega por e-mail um boleto de luz, água, internet ou de um fornecedor habitual, com aparência idêntica ao verdadeiro, mas com o código de barras alterado. O dinheiro vai para o golpista.

> **Como se defender:** Confira o **nome do beneficiário** e o **CNPJ** na tela do banco antes de confirmar. Na dúvida, emita a segunda via direto no site ou aplicativo oficial da empresa.

Falsa intimação judicial ou falso órgão público

Como funciona: Mensagem dizendo ser do Tribunal de Justiça, do Ministério Público, da Receita ou da Polícia, com um link para "ver o processo" ou um anexo. Como a Casa Lar lida com a Justiça da Infância, esse golpe parece muito verossímil.

> **Como se defender:** Órgãos públicos não cobram taxas por WhatsApp nem pedem senha. Confirme pelo telefone oficial do fórum ou da vara, que a coordenação já conhece — nunca pelo número que veio na mensagem.

"Troquei de número" / falso parente ou colega

Como funciona: Alguém usa a foto de um familiar, colega ou da coordenadora e diz que trocou de número. Logo depois pede um Pix urgente ou um pagamento "para resolver um problema".

> **Como se defender:** Ligue para o número **antigo** da pessoa ou faça uma pergunta que só ela saberia responder. Não transfira nada antes disso.

Clonagem do WhatsApp

Como funciona: O golpista pede "o código de 6 dígitos que chegou por SMS", fingindo ser de uma pesquisa, promoção, entrega ou cadastro. Com esse código, ele instala o WhatsApp da vítima em outro celular e passa a pedir dinheiro aos contatos.

> **Como se defender:** **Nunca** repasse códigos recebidos por SMS. Ative a confirmação em duas etapas (capítulo 5).

Falso doador ou falsa doação

Como funciona: Uma pessoa se apresenta como doador e pede dados bancários, cópia de documentos ou o pagamento de uma "taxa de liberação" para enviar a doação. Também existe o inverso: perfis falsos pedindo doações em nome da Casa Lar.

> **Como se defender:** Doação verdadeira não exige taxa. Documentos da instituição só são enviados por decisão da coordenação. Denuncie perfis falsos à rede social e avise a coordenação.

Falso comprovante de Pix

Como funciona: O "doador" ou "comprador" (num bazar, por exemplo) mostra um comprovante editado ou agendado, que nunca é pago.

> **Como se defender:** Só considere recebido quando o valor aparecer **no extrato** da conta da instituição.

Falsa central do banco ou falso suporte técnico

Como funciona: Ligação ou mensagem dizendo que há uma compra suspeita ou que o computador está com vírus. Pede para instalar um programa de "acesso remoto", informar senha, token ou fazer uma "transferência de segurança".

> **Como se defender:** Desligue. Banco não pede senha, não pede para transferir dinheiro "para proteger" e não pede para instalar programas. Ligue você mesma para o número do cartão.

CAPÍTULO 4

Como identificar uma mensagem falsa

Não é preciso ser especialista. Basta treinar o olhar para alguns sinais. Se você encontrar **um único** deles, trate a mensagem como suspeita até confirmar.

Sinais de alerta

- **Pressa ou ameaça**: prazos curtos, bloqueio de conta, multa, processo.
- **Remetente estranho**: endereço que imita o verdadeiro, com letras trocadas ou domínio diferente (ex.: *atendimento@bradesco-seguranca.com* ou *suporte@micros0ft.com*).
- **Pedido de senha, código, token ou dados bancários.** Empresas sérias não pedem isso por mensagem.
- **Link que não bate com o texto**: o texto diz um site, mas ao passar o mouse aparece outro endereço; links encurtados.
- **Anexo inesperado**, principalmente .zip, .rar, .exe, .html ou documentos que pedem para "habilitar conteúdo".
- **Saudação genérica** ("Prezado cliente") e erros de português.
- **Pedido de segredo**: "não comente com ninguém", "resolva só você".
- **Oferta boa demais**: prêmio, reembolso, doação grande com "pequena taxa".

Exemplo comentado

Veja um e-mail falso típico e os sinais que o denunciam:

De: Tribunal de Justiça <intimacao@tjsc-processos.online>
Assunto: URGENTE – Intimação eletrônica nº 0045871-22 – prazo de 24 horas

Prezado(a) responsável,

Consta em nosso sistema um processo em aberto em nome desta instituição. O não comparecimento implicará em bloqueio das contas. Para visualizar a intimação, acesse o documento em anexo e informe o CPF e a senha do gov.br do responsável legal.

Intimacao_0045871.html

1. O endereço não é do Tribunal (os endereços oficiais do TJSC terminam em *tjsc.jus.br*).

2. Urgência e ameaça de bloqueio.

3. Saudação genérica.

4. Pede CPF e senha do gov.br — nenhum órgão faz isso.

5. Anexo .html, formato muito usado para páginas falsas.

O método PARE – PENSE – CONFIRME

Etapa	O que fazer
PARE	Não clique, não responda, não pague. Nenhuma situação real se resolve em 5 minutos por uma mensagem.
PENSE	Eu esperava essa mensagem? Faz sentido esse pedido? Alguém está me pressionando?
CONFIRME	Entre em contato com a pessoa ou empresa por um canal que **você** já conhece: telefone oficial, aplicativo do banco, site digitado por você, ou falando com a coordenação pessoalmente.

Dica prática

No computador, passe o mouse sobre o link **sem clicar**: o endereço real aparece no canto da tela. No celular, pressione e segure o link para ver o endereço antes de abrir.

CAPÍTULO 5

Senhas e verificação em duas etapas

A senha é a chave da porta. Se for fraca, repetida ou compartilhada, qualquer vazamento em outro site abre também as contas da instituição.

Como criar uma senha forte e fácil de lembrar

Use uma **frase-senha**: três ou quatro palavras sem relação entre si, com um número e um símbolo. Exemplo de *estilo* (não use este!): **Janela!Café7Bicicleta**. Frases longas são mais seguras e mais fáceis de lembrar do que combinações curtas como *Casa@123*.

Evite	Prefira
Data de nascimento, nome de filhos, nome da instituição	Três ou quatro palavras aleatórias
A mesma senha em vários sites	Uma senha diferente para cada conta importante
Senha anotada em papel colado no monitor	Gerenciador de senhas (ex.: Bitwarden, gratuito)
Uma única senha compartilhada por toda a equipe	Cada funcionário com seu próprio usuário e senha

Verificação em duas etapas

A verificação em duas etapas (também chamada de **2FA** ou **autenticação em dois fatores**) pede, além da senha, um código gerado no seu celular. Assim, mesmo que o golpista descubra a senha, ele não consegue entrar. **É a proteção mais eficaz e barata que existe.** Ative, no mínimo, em:

- **WhatsApp:** Configurações → Conta → Confirmação em duas etapas → Ativar. Crie um PIN de 6 dígitos e cadastre um e-mail de recuperação.
- **E-mail** (Gmail, Outlook/Microsoft 365): nas configurações de segurança da conta, ative a verificação em duas etapas, de preferência com aplicativo autenticador.
- **Banco:** use o token do aplicativo oficial e nunca informe o código a ninguém.
- **Redes sociais da Casa Lar** (Instagram, Facebook): ative em Configurações → Segurança.

> **Atenção**
> O código da verificação em duas etapas é **pessoal e intransferível**. Se alguém pedir esse código — por qualquer motivo — é golpe.

Contas da instituição

- Quando um funcionário ou voluntário deixar a Casa Lar, **desative o acesso dele no mesmo dia** e troque as senhas que ele conhecia. A coordenação deve manter uma lista de quem tem acesso a cada sistema.
- O e-mail e o WhatsApp oficiais devem ter a recuperação de conta ligada a um número e a um e-mail **da instituição**, não de uma pessoa.

CAPÍTULO 6

Cuidado com os dados e a imagem das acolhidas

Este é o capítulo mais importante para uma casa de acolhimento. Muitas vezes o risco não vem de um golpista, mas de um descuido do dia a dia, feito com a melhor das intenções.

Nunca faça

- Publicar fotos, vídeos, nomes ou qualquer informação que identifique as meninas em redes sociais pessoais, status do WhatsApp ou grupos — nem de costas, nem com o rosto coberto, nem em datas comemorativas.
- Enviar documentos, relatórios ou fotos das acolhidas pelo seu WhatsApp ou e-mail pessoal.
- Comentar casos das acolhidas em grupos de mensagens, mesmo com colegas.
- Deixar papéis com dados das acolhidas sobre mesas, impressoras ou no lixo comum.

Sempre faça

- Use apenas os **canais oficiais** da Casa Lar para comunicar informações das acolhidas.
- Antes de enviar um e-mail para o Judiciário, Conselho Tutelar ou rede de proteção, **confira o destinatário** duas vezes.
- Ao sair do computador, bloqueie a tela: tecla **Windows + L**.
- Mantenha seu celular com senha ou biometria, principalmente se ele tem contato com assuntos da instituição.
- Picote ou triture papéis com dados pessoais antes de descartar.
- Em caso de dúvida sobre o que pode ou não ser compartilhado, pergunte à coordenação.

E as fotos das atividades?

Registrar momentos bonitos da rotina é natural. Mas, no caso de crianças e adolescentes em acolhimento, a divulgação pode revelar a localização delas a pessoas de quem foram afastadas por medida de proteção. Qualquer uso de imagem deve seguir a orientação da coordenação e da equipe técnica, que conhecem as determinações judiciais de cada caso. Na dúvida, **não publique**.

CAPÍTULO 7

Computadores, celulares e internet da instituição

Hábitos simples com os equipamentos reduzem muito o risco de vírus, sequestro de dados e invasões.

Tema	Boa prática
Atualizações	Aceite as atualizações do Windows, do celular e dos aplicativos. Elas corrigem falhas usadas por golpistas.
Antivírus	O Microsoft Defender, que já vem no Windows, é suficiente se estiver ativo e atualizado. Não instale “antivírus” oferecidos por janelas ou anúncios.
Programas	Instale programas apenas com autorização da coordenação e de fontes oficiais (site do fabricante, Microsoft Store, Google Play, App Store).
Pendrives	Não conecte pendrives encontrados ou de origem desconhecida.
Wi-Fi	Senha forte no Wi-Fi e, se possível, uma rede separada para visitantes e para os aparelhos das acolhidas.
Backup	Documentos importantes em pelo menos dois lugares (ex.: nuvem da instituição e um HD externo guardado em local seguro). Se um vírus sequestrar os arquivos, o backup salva a instituição.
Wi-Fi público	Evite acessar banco ou e-mail da instituição em redes abertas (shopping, rodoviária).

Regra 3-2-1 do backup

Mantenha **3** cópias dos arquivos importantes, em **2** tipos de armazenamento diferentes, sendo **1** delas fora da Casa Lar (por exemplo, na nuvem).

CAPÍTULO 8

Caí num golpe. E agora?

Qualquer pessoa pode cair em um golpe. O importante é **agir rápido e sem vergonha**: quanto antes o problema for comunicado, maiores as chances de reduzir o prejuízo. Ninguém deve ser culpado por avisar.

1. **Mantenha a calma e avise a coordenação imediatamente.** Não tente resolver sozinha.
2. **Não apague nada:** guarde prints das mensagens, e-mails, números de telefone e comprovantes. São provas.
3. **Se informou uma senha:** troque essa senha imediatamente, a partir de outro aparelho de confiança, e ative a verificação em duas etapas.
4. **Se clicou em um link ou abriu um anexo no computador:** desconecte-o da internet (cabo e Wi-Fi) e peça ajuda técnica antes de voltar a usá-lo.
5. **Se fez um Pix ou pagamento:** ligue para o banco na hora e peça a abertura do **MED – Mecanismo Especial de Devolução** do Pix. Quanto mais rápido, maior a chance de recuperar o valor.
6. **Se o WhatsApp foi clonado:** reinstale o aplicativo e entre de novo com o seu número; escreva para *support@support.whatsapp.com* relatando o caso e avise seus contatos para não atenderem a pedidos de dinheiro.
7. **Registre um Boletim de Ocorrência.** Em Santa Catarina, pode ser feito pela Delegacia Virtual da Polícia Civil, pela internet.
8. **Se dados das acolhidas ou de outras pessoas vazaram:** a coordenação deve avaliar a comunicação à ANPD (Autoridade Nacional de Proteção de Dados) e às pessoas afetadas, conforme a LGPD, e informar os órgãos da rede de proteção.

> **Para a coordenação**
>
> Tenha anotados, em papel, os telefones do gerente do banco, do suporte técnico e da Delegacia. Em um incidente, o computador ou o celular pode estar indisponível.

CAPÍTULO 9

Checklist da equipe e quiz de fixação

Imprima esta página e deixe perto dos computadores.

☐	Minha senha do e-mail e do WhatsApp é forte e não é usada em outro lugar.
☐	A verificação em duas etapas está ativa no meu WhatsApp e no meu e-mail.
☐	Eu nunca passo códigos recebidos por SMS para ninguém.
☐	Antes de pagar um boleto, confiro o beneficiário e o CNPJ na tela do banco.
☐	Confirmo pedidos de dinheiro por outro canal, mesmo quando vêm de conhecidos.
☐	Não publico nem envio fotos ou dados das acolhidas por canais pessoais.
☐	Bloqueio a tela (Windows + L) quando saio do computador.
☐	Aceito as atualizações do computador e do celular.
☐	Sei a quem avisar se eu cair em um golpe: a coordenação, imediatamente.

Quiz de fixação

1. Chega um SMS dizendo “Sua encomenda está retida, pague R$ 4,90 no link”. O que fazer?

a) Pagar, pois o valor é baixo

b) Responder pedindo mais informações

c) Ignorar e, se esperar uma encomenda, consultar pelo site oficial dos Correios

2. Uma colega manda mensagem de um número novo pedindo um Pix urgente. Qual a atitude correta?

a) Ligar para o número antigo dela ou confirmar pessoalmente antes

b) Fazer o Pix para ajudar

c) Pedir o comprovante depois

3. Alguém liga dizendo ser do WhatsApp e pede o código de 6 dígitos que chegou por SMS.

a) Informar, pois é do suporte

b) Informar só os 3 primeiros números

c) Nunca informar: é tentativa de clonar o WhatsApp

4. Qual destes endereços de e-mail é mais suspeito?

a) comunicacao@tjsc.jus.br

b) intimacao@tjsc-processos.online

c) Nenhum dos dois

5. Posso publicar no meu Instagram a foto de uma festa na Casa Lar com as meninas de costas?

a) Não. Sem orientação da coordenação, nenhuma imagem das acolhidas deve ser publicada

b) Sim, se estiverem de costas

c) Sim, se eu não marcar a Casa Lar

6. Fiz um Pix para um golpista. Qual o primeiro passo com o banco?

a) Esperar alguns dias para ver se o golpista devolve

b) Ligar imediatamente e pedir a abertura do MED (Mecanismo Especial de Devolução)

c) Apagar as mensagens para esquecer o assunto

Gabarito: 1-c · 2-a · 3-c · 4-b · 5-a · 6-b. Se a equipe acertou todas, ótimo! Se errou alguma, vale reler o capítulo correspondente.

REFERÊNCIA RÁPIDA

Contatos e canais úteis

Situação	Onde procurar
Registrar Boletim de Ocorrência	Delegacia Virtual da Polícia Civil de Santa Catarina (site oficial da PCSC) ou delegacia mais próxima
Pix enviado para golpista	Central de atendimento do próprio banco – pedir abertura do MED
Verificar contas ou chaves Pix abertas em seu nome	Registrato, do Banco Central (acesso pelo gov.br)
WhatsApp clonado	support@support.whatsapp.com e reinstalação do aplicativo com o seu número
Denunciar crimes na internet contra crianças e adolescentes	SaferNet Brasil – denuncie.org.br
Incidente com dados pessoais	ANPD – Autoridade Nacional de Proteção de Dados (gov.br/anpd)
Emergências	Polícia Militar – 190

Anote aqui os contatos internos:

Coordenação:	
Responsável pela informática / suporte técnico:	
Gerente do banco:	
Outro:	

Sobre este material

Este e-book foi elaborado voluntariamente, sem fins comerciais, como Atividade de Extensão do Curso Superior de Tecnologia em Gestão da Tecnologia da Informação da Universidade Paulista – UNIP, alinhado aos Objetivos de Desenvolvimento Sustentável da ONU nº 4 (Educação de qualidade), nº 10 (Redução das desigualdades) e nº 16 (Paz, justiça e instituições eficazes). Pode ser impresso e compartilhado livremente com a equipe da Casa Lar.

Referências: Lei nº 8.069/1990 (ECA); Lei nº 13.709/2018 (LGPD); Resolução CNE/CES nº 7/2018; Cartilha de Segurança para Internet – CERT.br (cartilha.cert.br); Banco Central do Brasil – Pix e MED.