# SEGURANÇA DIGITAL

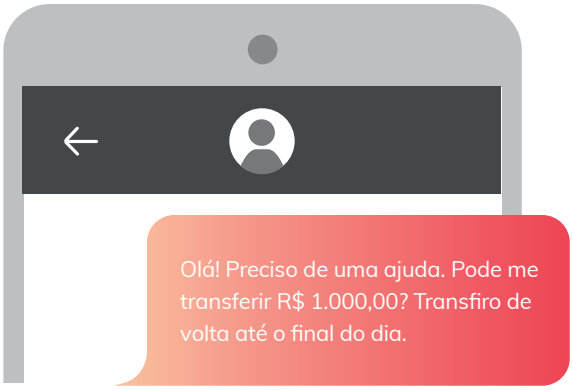
Um guia para se proteger dos golpes

Banco Daycoval

# PIX

**Simples, ágil e seguro.** Essas são características do novo sistema de transferências instantâneas, o PIX, porém, os fraudadores têm aplicado golpes de **"phishing"** para acessar contas, movimentar recursos e se aproveitam justamente da rapidez nas transações feitas por meio desse sistema.

**O meio principal para esses golpes tem sido o Whatsapp.** Por isso, desconfie de mensagens que peçam dinheiro pelo aplicativo ou por telefone, mesmo que sejam enviadas por números conhecidos Não compartilhe dados bancários ou pessoais por aplicativos de mensagens.




**Antes de efetivar uma transferência via Pix, o sistema mostra o nome completo, o banco e um trecho do CPF do destinatário.** Em alguns casos, a chave Pix é o próprio CPF. Essas informações ficam salvas no comprovante virtual da transação. Caso seja identificada alguma irregularidade na transação, a vítima poderá entrar em contato com o banco e bloquear a movimentação da conta.

# GOLPE DO WHATSAPP

Com o número telefônico da vítima e informações sobre seus hábitos de consumo – uma loja em que ela costuma comprar, por exemplo –, o criminoso entra em contato e se passa por funcionário dessa empresa para dizer que a pessoa tem direito a um **"cupom de desconto"**. A vítima recebe uma **mensagem por WhatsApp** e, ao clicar nela, dá ao golpista acesso a seus contatos.

**O criminoso dispara mensagens aos contatos solicitando transferências de valores.**

## GOLPE DO FALSO INVESTIMENTO

**O criminoso se passa por parceiro do banco e apresenta uma proposta tentadora de investimento.** O que ocorre é que a "oportunidade" só poderá ser "aproveitada" se a vítima depositar o dinheiro da aplicação em uma conta corrente informada pelo falso parceiro.

## GOLPE DA FALSA APROVAÇÃO DE CRÉDITO

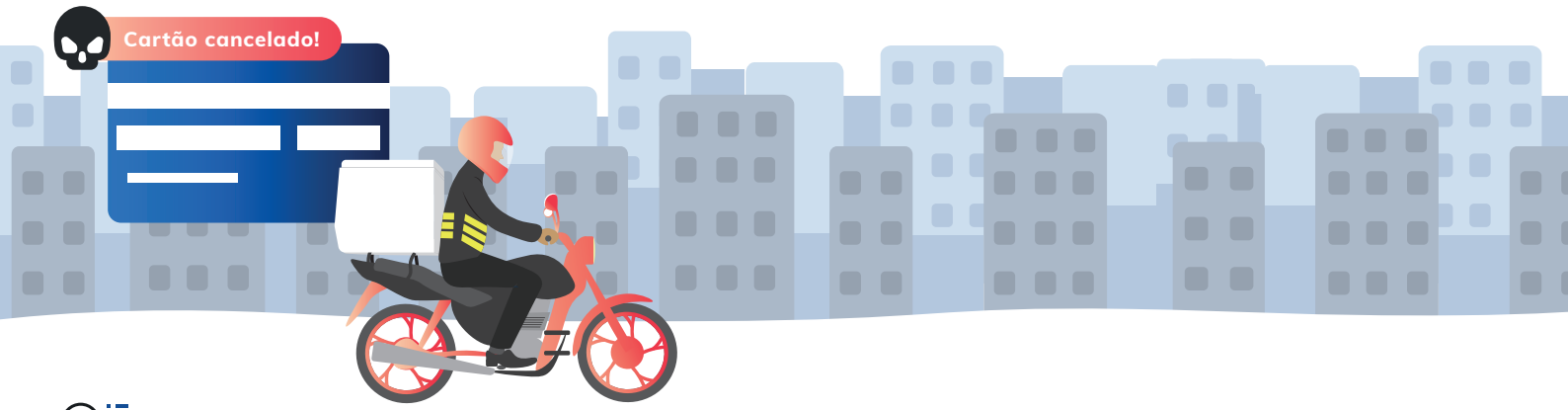
Nessa técnica, o golpista afirma ser um parceiro do banco e que entrou em contato para informar que o cliente tem um "crédito aprovado". **Para liberar o dinheiro, no entanto, é preciso "pagar uma taxa".**

## GOLPE DA FALSA CENTRAL OU FALSO FUNCIONÁRIO

**Um contato feito por uma falsa central telefônica do banco solicita os dados financeiros, a senha** e envia boletos para despesas que, na verdade, não existem.

## CARTÃO CLONADO, OU GOLPE DO MOTOBOY

O golpista finge ser da área de prevenção a fraudes do banco, **informa que o cartão do cliente está cancelado** e solicita os dados do cartão, como o código de segurança. **Em alguns casos, um motoboy é enviado para retirar o cartão** – daí o nome do golpe.



# E-MAILS E PÁGINAS FALSAS: ENTENDA O PHISHING

**O phishing é uma técnica usada por cibercriminosos para tentar obter informações confidenciais como nomes de usuário, senhas e detalhes de cartão de crédito.** A ação ocorre por meio de um "disfarce virtual", como um site falso de um banco ou um e-mail de uma entidade que parece confiável. Ao clicar nos links recebidos com as mensagens, a pessoa sem querer instala programas espiões em seus computadores e celulares, com os quais os criminosos acessam os dados.

**Para identificar o phishing fique atento a:**

O endereço do e-mail que enviou. Atenção para erros ortográficos e gramaticais

Logotipos fora do padrão

Solicitação de informações pessoais ou confidenciais


Endereço eletrônico ao qual remete, anexos (não abra) e também se há conteúdos de urgência

Além de e-mail, os criminosos têm aplicado o golpe por meio de **SMS, WhatsApp e Telegram**, por isso, **nada de acessar links enviados por canais suspeitos por meio dessas plataformas.**

# SEGURANÇA DIGITAL: AS ARMADILHAS DAS REDES SOCIAIS

Não é porque estamos fazendo uma ótima viagem de férias que tudo precisa ser registrado nas redes sociais. Mas, se a tentação de mostrar o passeio em uma selfie for muito grande, a imagem não precisa ser vista por quem não conhecemos. Esse cuidado também faz parte de nossa segurança financeira no ambiente digital.

O Daycoval apresenta, a seguir, dicas sobre como assegurar a privacidade de dados sem precisar abrir mão das redes sociais.

**1. Evite se expor demais:** Para não enfrentar dores de cabeça desnecessárias, evite compartilhar publicamente informações pessoais, financeiras e corporativas nas redes sociais. Passar a impressão de ostentação pode virar uma armadilha.

**2. Restrinja seu público:** Configurar a privacidade de suas postagens para que apenas pessoas realmente próximas possam vê-las é uma medida de reforço a sua segurança no ambiente digital.

**3. Cuidado com promoções on-line:** Nunca preencha suas informações pessoais em formulários de promoções sem verificar no site oficial da empresa se elas são, de fato, legítimas.

**4. Oriente seus familiares:** Os cuidados que você adotar têm que ser repassados também para a família.

**5. Testes do Facebook:** Com testes como: Quantos filhos você vai ter? Qual a cidade que você mais se identifica? Entre outras propostas, os testes de personalidade disponíveis nas redes sociais podem ocultar golpes de phishing, que visam roubar dados de usuários. Muitas vezes eles burlam as políticas de segurança de dados dos aplicativos de redes sociais. Por isso, evite acessar esses testes.

**6. Atenção para as ações solidárias:** Muitas vezes são golpes para a captação de dinheiro indevidamente e com possíveis casos de fuga de dados.

# SENHAS E AUTENTICAÇÃO: O QUE FAZER (E O QUE NÃO FAZER)

As transações financeiras no ambiente digital são práticas e também seguras, o que não significa que se pode relaxar. A seguir, o Daycoval apresenta um guia definitivo sobre como proteger sua senha bancária e como reforçar a segurança de seus dados por meio da chamada autenticação de dois fatores.

**1. A regra de ouro:** não se compartilha senha: Jamais compartilhe sua senha bancária. Não anote sua senha em caderno ou agendas, não a salve no celular ou no computador nem a fale, escreva ou envie por e-mail, WhatsApp ou mensagens em redes sociais. Como parte dessa regra geral, lembre-se que nenhum banco solicita senhas de clientes;

**2. Troque sua senha sempre:** Substitua sua senha com regularidade – de dois em dois meses, por exemplo. A mudança também precisa ser feita sempre que você desconfiar que ela foi comprometida.

**3. Cada serviço, uma senha:** Se você utiliza a mesma senha para seu internet banking, seu e-mail e sua conta no Instagram, mude as três imediatamente. Cada serviço tem que ter uma senha própria.

**4. Crie senhas complexas:** As senhas ficam mais seguras quando são compostas por letras, números e, sempre que possível, também por caracteres especiais. Utilize gerenciadores de senhas que criptografam suas credenciais e geram senhas complexas e aleatórias.

**5. Duplo fator de autenticação, um aliado:** Para reforçar a segurança, use sempre a chamada autenticação de dois fatores (ou verificação em duas etapas), que inclui uma segunda camada de autenticação para garantir o acesso. Certifique-se de que você habilitou o recurso em todas as aplicações que o oferecem, como Instagram, LinkedIn e Facebook.

**6. Acesso ao celular:** Configure uma senha para acessar seu smartphone – e não use PIN ou padrão de desenho. Se o seu aparelho permite biometria ou reconhecimento facial, utilize esses recursos.