MPSP

MINISTÉRIO PÚBLICO
DO ESTADO DE SÃO PAULO

Guia de Sobrevivência Digital : Proteja seu Dinheiro

Uma iniciativa do
Ministério Público do Estado de São Paulo

Bem-vindo ao guia

Esta cartilha foi criada com uma linguagem simples e direta para te ensinar a reconhecer os golpes mais comuns e, principalmente, como evita-los.

MPSP

Uma iniciativa do
Centro de Apoio do Consumidor do
Ministério Público do Estado de São Paulo

GUIA DE SOBREVIVÊNCIA DIGITAL: PROTEJA-SE DE GOLPES

01. Golpe do WhatsApp (Perfil Falso)

O que é:

Um criminoso usa **sua foto e um número novo** para se passar por você.

Como acontece:

Ele envia mensagens para seus **contatos** dizendo que **"mudou de número"** e que precisa pagar uma **conta urgente**.

Sinal de Alerta:

Pedido de dinheiro por mensagem, mesmo que a foto seja de um familiar.

Como se proteger:

Nunca transfira valores sem antes fazer uma ligação comum ou de vídeo para confirmar.

GUIA DE SOBREVIVÊNCIA DIGITAL: PROTEJA-SE DE GOLPES

02. Falsa Central Telefônica

O que é:

Um criminoso **finge ser do suporte do seu banco**.

Como acontece:

Eles ligam sobre "**compra suspeita**" e pedem para confirmar dados ou digitar senha.

Sinal de Alerta:

Bancos **nunca** ligam pedindo senhas, códigos de token ou transferências.

Como se proteger:

Desligue imediatamente. Use o número oficial atrás do seu cartão.

GUIA DE SOBREVIVÊNCIA DIGITAL: PROTEJA-SE DE GOLPES

03. Phishing (Links Falsos)

O que é:
Mensagens de texto ou e-mail que roubam seus dados.

Como acontece:
Envia avisos urgentes (Serasa, Correios, Receita) com links para sites falsos.

Sinal de Alerta:
Cria senso de desespero e usa links com letras estranhas.

Como se proteger:
Não clique! Acesse direto o app oficial ou site pelo seu navegador.

GUIA DE SOBREVIVÊNCIA DIGITAL: PROTEJA-SE DE GOLPES

04. Falso Motoboy

O que é:
O criminoso vai até a sua casa buscar o seu cartão físico.

Como acontece:
Dizem que seu cartão foi 'clonado' e um motoboy do banco vai buscá-lo para perícia.

Sinal de Alerta:
Bancos **JAMAIS** mandam buscar cartões, mesmo que estejam 'cortados'.

Como se proteger:
Destrua o chip do cartão. Nunca o entregue a estranhos.

GUIA DE SOBREVIVÊNCIA DIGITAL: PROTEJA-SE DE GOLPES

05. Pix Agendado

O que é:
O uso de um comprovante de "futuro pagamento" para enganar vendedores.

Como acontece:
O golpista agenda um Pix para uma data futura, tira print e envia. Assim que recebe o produto, ele cancela.

Sinal de Alerta:
Comprovantes que mostram a palavra **"Agendado"** em vez de "Transferência Concluída".

Como se proteger:
Só entregue produtos após conferir no extrato se o dinheiro caiu.

GUIA DE SOBREVIVÊNCIA DIGITAL: PROTEJA-SE DE GOLPES

06. QR Code Falso

O que é:
Códigos de pagamento alterados para desviar o seu dinheiro.

Como acontece:
Criminosos colam adesivos com QR Codes próprios sobre o código real de lojistas ou enviam boletos falsos.

Sinal de Alerta:
Na tela de confirmação do Pix, o nome do recebedor é diferente da loja ou empresa que você está pagando.

Como se proteger:
Sempre confira o nome e o CPF/CNPJ do destino antes de digitar sua senha.

MPSP MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO
Informação é sua melhor defesa

GUIA DE SOBREVIVÊNCIA DIGITAL: PROTEJA-SE DE GOLPES

07. Falso Boleto / DARF Falsa

O que é:
Boletos de cobrança reais (IPVA, condomínio, luz) com dados alterados.

Como acontece:
Você recebe um boleto por e-mail ou WhatsApp que parece oficial, mas o dinheiro vai para outra conta.

Sinal de Alerta:
Erros de digitação, logotipos borrados ou quando o beneficiário no banco é uma pessoa física.

Como se proteger:
Utilize o DDA (Débito Direto Autorizado) no seu banco para pagar contas oficiais.

GUIA DE SOBREVIVÊNCIA DIGITAL: PROTEJA-SE DE GOLPES

08. Golpe da Mão Fantasma

O que é:
O criminoso assume o controle remoto do seu celular para limpar suas contas.

Como acontece:
Por telefone, convencem você a baixar um "aplicativo de segurança". Esse app dá ao golpista acesso total.

Sinal de Alerta:
Pedidos para instalar aplicativos como *AnyDesk* ou *TeamViewer* para "suporte bancário".

Como se proteger:
O banco nunca pede para você instalar aplicativos de terceiros. Se pedirem, desligue.

GUIA DE SOBREVIVÊNCIA DIGITAL: PROTEJA-SE DE GOLPES

09. Falsa Venda (E-commerce)

O que é:

Produtos com preços irreais em sites falsos ou anúncios de redes socials.

Como acontece:

O produto aparece com até 90% de desconto. Após o pagamento, o site some e o produto nunca chega.

Sinal de Alerta:

Preços "milagrosos" e sites que só aceitam Pix ou boleto como pagamento.

Como se proteger:

Verifique a reputação do site em plataformas confiáveis, como Reclame Aqui e Procon e desconfie de ofertas excessivamente baratas.

10. Falsos Investimentos / Pirâmides

O que é:
Promessas de lucro alto, rápido e sem risco.

Como acontece:
Convites para investir em criptomoedas desconhecidas ou cumprir "tarefas online" em troca de dinheiro.

Sinal de Alerta:
Promessa de lucro garantido e necessidade de indicar novos membros para ganhar.

Como se proteger:
Não existe lucro alto sem risco. Invista em corretoras registradas na CVM.

GUIA DE SOBREVIVÊNCIA DIGITAL: PROTEJA-SE DE GOLPES

11. Troca de Cartão

O que é:
O criminoso troca o seu cartão original por um idêntico presencialmente.

Como acontece:
Ao pagar, o vendedor distrai você e devolve um cartão idêntico, mas de outra pessoa. Ele já viu a senha.

Sinal de Alerta:
O vendedor passa o cartão várias vezes ou pede para você repetir a senha em máquinas com o visor danificado.

Como se proteger:
Sempre confira o seu nome no cartão e nunca o entregue a estranhos.

12. Devolução de Empréstimo

O que é:

O golpista deposita um valor na sua conta e pede a devolução.

Como acontece:

Um valor cai na sua conta (geralmente um consignado não autorizado). O golpista liga e pede devolução em conta de terceiro.

Sinal de Alerta:

Dinheiro "inesperado" que cai na conta e alguém pressionando para você transferir de volta.

Como se proteger:

O banco **nunca** pede devolução em conta de terceiro. Se receber um consignado, entre em contato com o seu banco.

MPSP
MINISTÉRIO PÚBLICO
DO ESTADO DE SÃO PAULO

Guia de Sobrevivência Digital

DESCONFIE, CONFIRME, PROTEJA SEU DINHEIRO

DESCONFIE SEMPRE de:

- Ofertas "boas demais para ser verdade" e a reputação das empresas que fazem essas ofertas
- Mensagens urgentes de "atendentes" de banco ou cartões, pedindo dados, códigos ou senhas
- Pedidos urgentes de pagamento de conta, transferencias ou Pix, mesmo de parentes ou amigos.
- Mensagens que mandam clicar em "links" ou QR codes duvidosos, ou que mandam baixar aplicativos desconhecidos

SEMPRE CONFIRME: A identidade da pessoa que te mandou uma mensagem urgente

- Os dados do destinatário do pix/transferência, e o valor exato
- Os dados do destinatário de boletos/QR Codes de pagamentos, assim como o valor e banco recebedor
- A reputação da empresa que faz a oferta e o valor do produto

SE CAIR NO GOLPE: Faça Boletim de ocorrência

- Ligue urgente para a sua agência/gerente bancário e tente o estorno de transferências/pix
- Ligue para o número do verso do seu cartão de crédito

Outras dicas:

- Portal da Cidadania Digital do Governo Federal: https://www.gov.br/gsl/pt-br/seguranca-da-informacao-e-cibernetica/cidadania-digital
- Procon SP: https://www.procon.sp.gov.br/