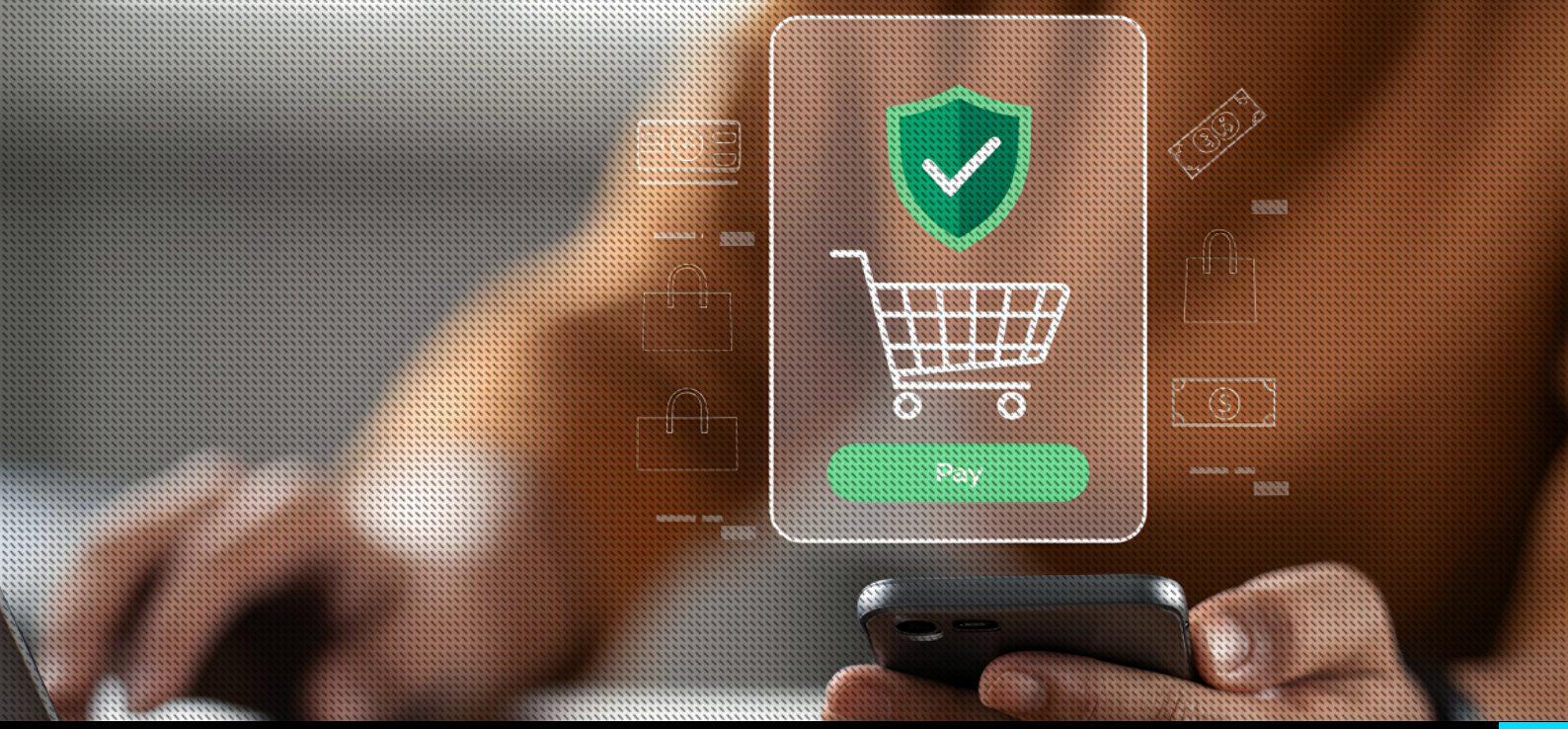


CUIDADOS ESSENCIAIS COM GOLPES DIGITAIS NA BLACK FRIDAY E NAS FESTAS DE FIM DE ANO

Entenda como se proteger dos ataques mais comuns da temporada.

ostec
Segurança digital de resultados

AVISO DE DIREITOS E USO

POR QUE ESTE MATERIAL É IMPORTANTE?

Novembro marca o início da temporada de grandes promoções: Black Friday, Cyber Monday e as compras de fim de ano. É um período de euforia, pressa e consumo digital intenso.

Mas, enquanto consumidores buscam os melhores preços, cibercriminosos aproveitam a oportunidade para capturar algo muito mais valioso: seus dados.

Com técnicas cada vez mais sofisticadas, eles se aproveitam da distração e da urgência para aplicar golpes. Essa combinação faz do fim de ano o momento perfeito para ataques de phishing, roubo de credenciais, instalação de malwares e vazamento de informações corporativas.

A TEMPORADA DOS GOLPES

Durante a Black Friday e as festas de dezembro, o número de fraudes online cresce consideravelmente.

Mensagens falsas imitando lojas conhecidas, promoções irresistíveis enviadas por e-mail e links que prometem descontos milagrosos compõem um cenário de armadilhas digitais cuidadosamente construído para parecer legítimo.

Essas campanhas fraudulentas são, muitas vezes, tão bem elaboradas que até usuários atentos podem ser enganados. Um único clique pode direcionar para sites clonados, induzir o download de arquivos maliciosos ou capturar informações financeiras e senhas.

O problema se agrava quando essas ações ocorrem em equipamentos corporativos. O uso de notebooks, celulares e redes da empresa para compras pessoais pode abrir brechas de segurança que comprometem não apenas o colaborador, mas todo o ambiente de TI da organização.

RISCO PARA AS EMPRESAS

É comum que colaboradores acreditem que comprar algo rápido durante o expediente seja inofensivo. Porém, **basta um acesso a um site falso para permitir a entrada de malwares, keyloggers ou até ransomware na rede corporativa.**

Quando o e-mail institucional é usado para cadastros pessoais, cresce o risco de exposição de credenciais, spam e ataques direcionados. Extensões de navegador e aplicativos suspeitos também podem coletar dados sigilosos sem que o usuário perceba.

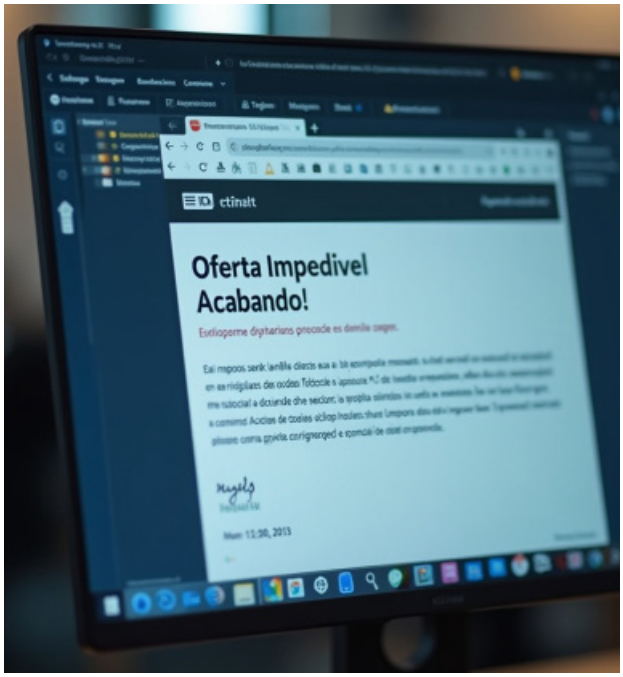
Em um simples clique, um desconto duvidoso pode se transformar em prejuízo financeiro, paralisação de sistemas e danos à reputação da empresa.

GOLPES MAIS FREQUENTES NESSA ÉPOCA

PHISHING

O phishing é o golpe mais recorrente neste período. Criminosos enviam mensagens falsas que imitam comunicações legítimas de lojas, bancos, transportadoras ou plataformas de pagamento. O objetivo é fazer o usuário clicar em um link malicioso e fornecer informações sigilosas, como senhas, CPF ou dados de cartão.

Essas mensagens geralmente apelam para a urgência, "sua entrega foi bloqueada", "sua compra será cancelada", "oferta por tempo limitado". Mesmo com visuais sofisticados, há sinais de alerta: erros de ortografia, endereços de remetente estranhos e links encurtados.

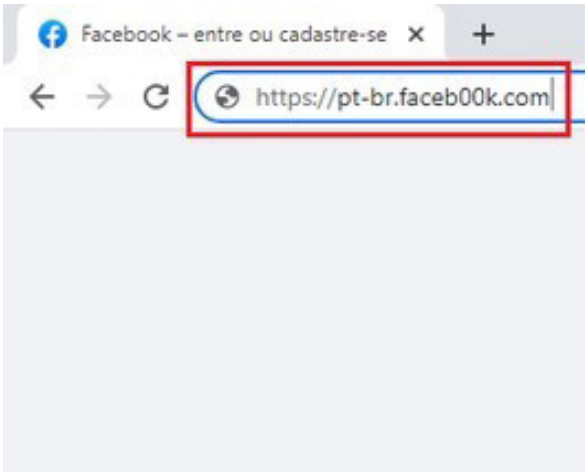


A recomendação é clara: nunca clique em links recebidos por e-mail ou mensagem. Se quiser confirmar a informação, digite o endereço da loja diretamente no navegador.

SITES CLONADOS

Os sites falsos, ou clonados, são uma das armadilhas mais perigosas da Black Friday. Criminosos criam páginas idênticas às de grandes lojas, reproduzindo cores, logotipos e até falsos certificados de segurança.

A diferença está em detalhes sutis do endereço: um caractere trocado **(amaz0n.com)**, um domínio alternativo **(.net em vez de .com)** ou subdomínios enganosos **(loja.oficial.promocao.com)**.



Ao efetuar uma compra nesses sites, o usuário entrega seus dados diretamente aos golpistas.

Por isso, **verifique sempre o domínio oficial e a presença do cadeado de segurança (HTTPS) — embora não seja uma garantia absoluta, é o primeiro passo de verificação. navegador.**

CUPONS E BRINDES FALSOS

Durante o período de ofertas, é comum receber links oferecendo cupons de desconto ou brindes gratuitos. As mensagens, muitas vezes compartilhadas em grupos ou redes sociais, pedem que o usuário preencha um formulário ou envie o link a amigos para liberar o benefício.

O que parece uma boa oportunidade é, na verdade, uma estratégia para coletar dados pessoais, instalar aplicativos falsos ou redirecionar para páginas maliciosas.

Desconfie de ofertas excessivamente vantajosas ou que exijam compartilhamento para liberar o prêmio, lojas legítimas não adotam esse tipo de prática.

GOLPES EM REDES SOCIAIS

As redes sociais também são palco para fraudes. Golpistas criam perfis falsos de lojas e influenciadores, muitas vezes com anúncios pagos para reforçar a credibilidade.

Esses perfis divulgam promoções relâmpago e direcionam usuários para sites fraudulentos.

Antes de comprar por um link no Instagram, Facebook ou TikTok, certifique-se de que o perfil é verificado, observe o histórico de publicações e os comentários. Perfis falsos geralmente têm poucas interações e conteúdo recente.

Mesmo em anúncios patrocinados, prefira acessar o site digitando o endereço diretamente no navegador.

RASTREAMENTO FALSO DE ENCOMENDAS

Outro golpe recorrente envolve mensagens falsas de rastreamento. Criminosos enviam SMS ou mensagens em aplicativos dizendo que houve um problema na entrega e solicitam que o usuário clique em um link para confirmar dados.

Esses links instalam malwares ou redirecionam para páginas de roubo de informações bancárias.

Essas mensagens geralmente vêm de números desconhecidos e apresentam erros de digitação ou formatação.

É importante lembrar que transportadoras e e-commerces não pedem atualização de dados via SMS ou WhatsApp.

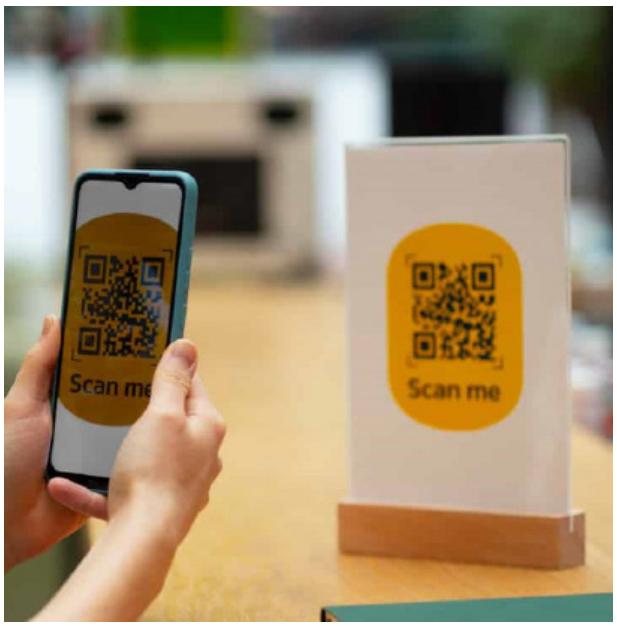
Em caso de dúvida, acesse o site oficial da loja ou da transportadora e insira o código de rastreio manualmente.

GOLPES QUE VISAM ROUBAR DINHEIRO: O PERIGO DOS PAGAMENTOS RÁPIDOS

Além de sites clonados e phishing, há uma categoria de fraudes muito direta e visível nesta época: golpes cujo objetivo é fazer a vítima transferir dinheiro imediatamente, geralmente por PIX, boleto ou pagamento via QR Code. Essas fraudes exploram a pressa do consumidor, ofertas chamativas e a confiança nas interfaces de pagamento.

Geralmente, funciona da seguinte maneira: Os criminosos criam anúncios atraentes no Instagram, Facebook e marketplaces oferecendo produtos reais, às vezes imagens roubadas de lojas legítimas, mas direcionam o comprador para um site alternativo ou para um contato de venda que pede pagamento por PIX ou boleto. O valor parece muito baixo e a urgência é legítima: **“só hoje”**, **“última unidade”**. Quando o comprador realiza o PIX para a chave informada ou paga o boleto, o dinheiro vai para uma conta controlada pelo golpista e desaparece. Como PIX e boletos são métodos de liquidação rápida, a reversão do pagamento é difícil ou impossível sem ação imediata do banco.

Outra variação comum é o **QR Code falso**: o golpista compartilha um QR que, ao ser lido, direciona para uma chave PIX que parece ser a da loja, mas não é. QR codificados em imagens ou páginas HTML podem ocultar chaves diferentes daquelas esperadas. Também há casos de boletos falsos cuja linha digitável foi alterada, na aparência é um boleto legítimo, mas o beneficiário final é outro.

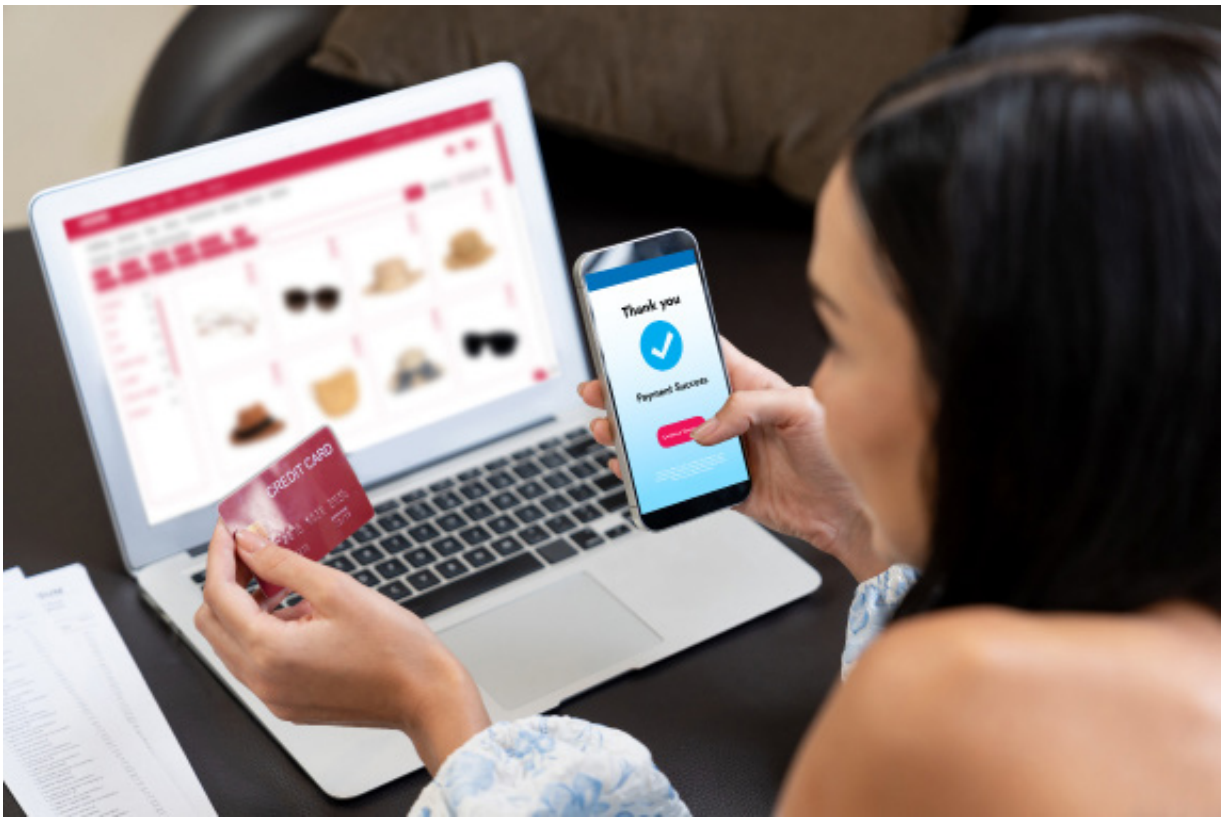


COMO IDENTIFICAR ESSES GOLPES

- Preço muito abaixo do mercado, combinado com pressão por pagamento imediato, é um sinal clássico;
- Pedidos de pagamento por PIX para pessoa física (CPF) em vez de conta empresarial ou checkout da loja merecem desconfiança;
- Anúncios que redirecionam para sites com layout simples, sem checkout seguro, ou que instruem a enviar comprovante por WhatsApp são suspeitos;
- QR Codes recebidos por mensagem ou redes sociais devem ser tratados com cautela, verifique a chave PIX exibida pelo seu aplicativo bancário antes de confirmar.

O QUE FAZER ANTES DE PAGAR

Procure sempre o canal oficial da loja: prefira o checkout do site oficial ou marketplaces conhecidos, que oferecem meios de pagamento com proteção ao comprador. Se o vendedor pedir PIX, verifique se a chave pertence à empresa, pesquise o CNPJ, confirme o celular ou e-mail no site oficial, e desconfie de instruções para "enviar comprovante e liberar produto". Para QR Codes, abra a leitura pelo app do seu banco e confirme a chave exibida; não confie apenas na imagem. No caso de boleto, confira a linha digitável e, se houver dúvida, prefira gerar o boleto direto pelo site oficial.



O QUE FAZER CASO VOCÊ TENHA SIDO VÍTIMA DE UM Ggolpe

A rapidez faz diferença. Contate imediatamente o banco ou a instituição financeira para tentar bloquear ou rastrear a transação. Registre um B.O. e reúna comprovantes (capturas de tela, conversas, comprovante de pagamento).

Caso isso tenha ocorrido em ambiente de trabalho: Notifique a área de segurança ou financeira da empresa, especialmente se a transação envolveu cartão/conta corporativa, para que medidas internas de contenção sejam tomadas. Em seguida, avalie se há necessidade de trocar senhas, revisar acessos e comunicar clientes/fornecedores, quando aplicável.

COMO SE PROTEGER DE GOLPES NESSA ÉPOCA

A prevenção começa com atitudes simples:

- Desconfie de promoções milagrosas, evite clicar em links recebidos por e-mail e confirme sempre se o site é realmente o oficial.
- Antes de inserir dados pessoais, verifique o uso do HTTPS e se o endereço corresponde exatamente ao domínio da loja.
- Evite utilizar dispositivos ou redes corporativas para compras pessoais.
- Mantenha sistemas e antivírus atualizados, use autenticação multifator e jamais salve senhas nos navegadores da empresa.
- Ao usar redes Wi-Fi públicas, redobre a atenção — elas podem facilitar a interceptação de dados. Prefira conexões privadas e seguras.

O BÁSICO PARA SE MANTER SEMPRE SEGURO

NO AMBIENTE CORPORATIVO

- Use equipamentos corporativos apenas para fins profissionais.
- Evite acessar sites de compras, bancos e redes sociais durante o expediente.
- Nunca use o e-mail da empresa para cadastros pessoais.
- Não salve senhas em navegadores corporativos.
- Mantenha antivírus e sistemas atualizados.

NO AMBIENTE PESSOAL

- Compre apenas em sites oficiais e conhecidos.
- Prefira cartões virtuais e meios de pagamento seguros.
- Habilite autenticação multifator (MFA).
- Evite Wi-Fi público para realizar compras ou acessar contas.
- Fique atento a mensagens urgentes ou pedidos de atualização de dados.

CULTURA DE SEGURANÇA NAS EMPRESAS: O MELHOR INVESTIMENTO

Mais do que antivírus, firewalls e políticas de acesso, a verdadeira defesa de uma empresa está nas pessoas que fazem parte dela.

A cultura de segurança nasce quando cada colaborador entende que suas ações — um clique, um download, um cuidado — podem proteger ou expor toda a organização.

Durante períodos como a Black Friday e as festas de fim de ano, em que a pressa e a empolgação se misturam às boas intenções, a atenção digital se torna essencial.

SEGURANÇA NÃO É BARREIRA, É HÁBITO.

Assim como trancamos as portas antes de sair de casa, devemos aprender a proteger nossos dados antes de navegar ou comprar online.

Empresas que promovem conscientização contínua e mantêm um diálogo aberto sobre boas práticas fortalecem a confiança interna e reduzem drasticamente o risco de incidentes.

Quando a segurança é encarada como atitude coletiva, todos saem ganhando — a empresa, o time e o próprio usuário.

Construir uma cultura de segurança é um investimento que se multiplica: protege dados, fortalece marcas e preserva relações.

E, diferente das promoções de novembro, ***essa cultura vale o ano inteiro.***

NOSSO COMPROMISSO COM A CIBERSEGURANÇA

Fundada em 2005, em Santa Catarina, a OSTEC é uma empresa referência e com ampla experiência no setor de cibersegurança, desenvolvendo soluções próprias, fornecendo serviços e atuando com portfólio de parceiros de mercado.

Com mais de 2 mil clientes e atuação transversal em diferentes segmentos, possui operações no Brasil e no Chile.

Por meio do Grupo OSTEC, forma um ecossistema one stop shop de soluções de cibersegurança reconhecidas com os selos ISO 27001 e 27701 e que engloba as empresas Dédalo, Enorx, Deconve e Seguridad América.

DÊ O PRÓXIMO PASSO PARA A RESILIÊNCIA CIBERNÉTICA

Transforme o risco da sua cadeia de suprimentos em resiliência gerenciada.

Converse com um especialista OSTEC:

contato@ostec.com.br

www.ostec.com.br

Siga nossas redes sociais:

/ostec-security

@ostecsecurity


ostec
Segurança digital de resultados