Phishing:

é tudo sobre
o seu clique!

dialogando
vivo

ÍNDICE

Na internet circulam informações de qualquer tipo e origem, inclusive falsas e maliciosas. Acreditar cegamente em tudo que recebe ou acessa facilita a ação de golpistas, que estão sempre criando novos truques para enganar e tirar vantagem das pessoas.

Não se deixe enganar! Veja aqui como se proteger do **phishing** e seus derivados.

O Dialogando

Desde 2016, o portal Dialogando tem como objetivo promover a discussão sobre o uso responsável da tecnologia. Com o respaldo da Vivo, o portal ocupa um espaço que nenhuma empresa de telecomunicações conquistou, e o faz por meio da abordagem educativa de temas relacionados ao uso consciente da internet e seus impactos na vida das pessoas e da sociedade. Presente em 10 países, com versões em português e espanhol, o Dialogando aborda a tecnologia em 5 pilares diferentes: Sustentabilidade, Educação, Inovação, Segurança e Comportamento.

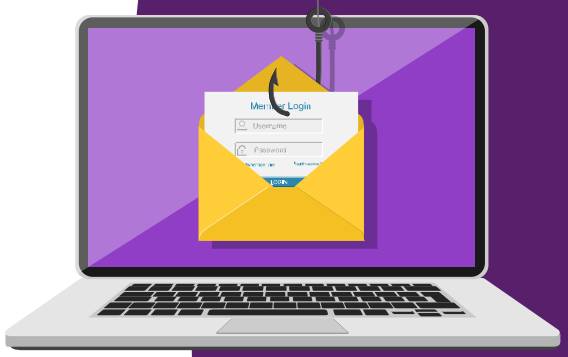
- Sustentabilidade
- Educação
- inovação
- Segurança
- Comportamento

CENÁRIO

Apesar da popularidade dos programas maliciosos no setor de cibersegurança, a maior ameaça na América Latina é o phishing — mensagens enviadas por e-mail, SMS e — principalmente — por redes sociais e por aplicativos de mensagem como o WhatsApp.

Nos primeiros oito meses de 2022, foram bloqueados 38 milhões de acessos a links fraudulentos. Este número representa 75% das tentativas de ataques de phishing em 2021, quando se registrou um total de 52 milhões.

O Brasil ainda é o país mais atacado na América Latina, seguido pelo Equador — ambos estão na lista mundial dos 10 países mais atacados por phishing e ocupam, respectivamente, a 6ª e a 8ª posições. Eles são seguidos por Peru (33°), Colômbia (37°), Chile (48°), Panamá (51°), Guatemala (61°), Paraguai (65°) e México (71°).



Mas o que é o phishing, afinal?

Um tipo de fraude em que cibercriminosos tentam obter dados pessoais e financeiros de um usuário por meio do envio de mensagens eletrônicas que:

- Tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um site popular;
- Procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;
- Informam que a não execução dos procedimentos pedidos pode acarretar sérias consequências, como a inscrição em serviços de proteção ao crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito;
- Tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas que tentam se passar pela página oficial de uma instituição.

Mas como?

Os golpistas instalam códigos maliciosos nesses ambientes virtuais, projetados para coletar informações sensíveis de suas iscas.

Pausa para a reflexão!

Quantos segundos você levaria para apertar no link de um e-mail com esta mensagem no campo assunto?

iPhone 12: SÓ HOJE por R$ 799,99.

Sentiu que há uma oportunidade muito tentadora em qualquer mensagem eletrônica? **FUJA!**

Mais situações!

Páginas falsas de comércio eletrônico ou Internet Banking:

• Você recebe um e-mail em nome de um site de comércio eletrônico ou instituição financeira. Ao clicar, você é direcionado para um site falso, muito semelhante ao verdadeiro;

• Na página fraudulenta, são solicitados seus dados pessoais e financeiros;

• Você entrega tudo e pronto. Fica à mercê dos cibercriminosos.

Páginas falsas de redes sociais ou de companhias aéreas:

• Você recebe uma mensagem contendo um link para o site da rede social ou da companhia aérea que utiliza;

• Ao clicar, é direcionado para uma página Web falsa, onde é solicitado o seu usuário e senha;

• Ao fornecer seus dados, eles serão enviados aos golpistas, que passarão a ter acesso ao site e poderão efetuar ações em seu nome.

Mensagens contendo formulários:

• Você recebe uma mensagem eletrônica contendo um formulário com campos para a digitação de dados pessoais e financeiros;

• A mensagem solicita o preenchimento do formulário e apresenta um botão para confirmar o envio das informações;

• Ao preencher os campos e confirmar o envio, seus dados são transmitidos para os golpistas.

Mensagens contendo links para códigos maliciosos:

• Você recebe um e-mail que tenta induzi-lo a clicar em um link, para baixar e abrir/executar um arquivo;

• Ao clicar, é apresentada uma mensagem de erro ou uma janela pedindo que você salve o arquivo;

• Após salvar e executar o arquivo, será instalado um código malicioso em seu computador, que abrirá as portas de sua máquina para os golpistas.

Solicitação de recadastramento

• Você recebe uma mensagem, supostamente enviada pelo grupo de suporte da instituição de ensino que frequenta ou da empresa em que trabalha;

• Ela informa que o serviço de e-mail está passando por manutenção e que é necessário o recadastramento;

• Para isto, é preciso que você forneça seus dados pessoais, como nome de usuário e senha;

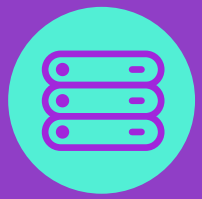
• Você fornece e pronto. Virou só mais uma vítima.

Como identificar um phishing?

a) Atente-se ao remetente. É de um contato confiável?

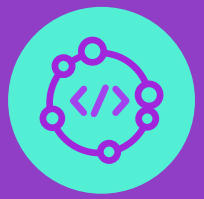
b) Para quem foi enviado? "Caro cliente".

c) Erros de português são muito comuns.



d) Ilumine o link, sem clicar, e identifique a URL.

e) Utiliza um tom de urgência ou de uma promoção imperdível.



f) Anexos executáveis .exe ou .html.

g) Identidade visual não condizente com a da marca.

h) Site da marca não informa sobre a promoção.

Perceba, no ítem "G", que a nuance é discreta. No exemplo, mostramos um caso em que os golpistas teriam tentado falsificar um site da própria Vivo. Só que a logo nem é mais usada pela companhia.

QR Codes

Há códigos QR maliciosos, usados para direcionar usuários para páginas falsas ou com malware, a fim de capturar dados e cometer fraudes. Desconfie até mesmo de mensagens enviadas por "conhecidos" e, se necessário, contate quem supostamente a enviou, usando outro meio de comunicação.

#FicaAdica:

Só leia códigos QR se tiver certeza de que a fonte é confiável!

QUESTIONE SE O CONTEÚDO FAZ SENTIDO!

Pergunte-se, por exemplo:

- Tenho conta neste banco?
- Esse é o contato que uso com esta instituição?
- O valor da cobrança confere?
- Por que antecipar o pagamento e não descontar no final?

SUSPEITE

Desconfie de mensagens com temas cotidianos, como:

- Recadastramento de token;
- Cancelamento de CPF;
- Débitos pendentes;
- Oferta de emprego;
- Pontos ou bônus a vencer.

Atenção aos temas da vez!

Para atrair vítimas, oportunistas exploram assuntos de destaque do momento, como:

- Imposto de Renda;
- Eleições;
- Copa do Mundo;
- Acontecimentos que geram comoção, como desastres e doenças graves;

Não faça

o que pede a mensagem. Na dúvida, contate a instituição usando um canal oficial!

#FicaAdica:

busque informações somente em fontes oficiais e certifique-se antes de fazer pagamentos e doações.

PREVINA-SE!

• Fique atento a mensagens recebidas em nome de alguma empresa que tente induzi-lo a fornecer informações, instalar/executar programas ou clicar em links;

• Questione-se por que instituições com as quais você não tem contato estão te enviando mensagens. Exemplo: se você não tem conta em um determinado banco, não há motivo para recadastrar dados ou atualizar módulos de segurança;

• Desconfie de mensagens que apelem demais pela sua atenção e que, de alguma forma, o ameacem, caso você não execute os procedimentos descritos;

• Não considere que uma mensagem é confiável com base na confiança que você deposita em seu remetente. Ela pode ter sido enviada por contas invadidas, de perfis falsos;

• Seja cuidadoso ao acessar links. Procure digitar o endereço diretamente no navegador Web;

• Verifique o link apresentado na mensagem. Golpistas costumam usar técnicas para ofuscar o link real para o phishing. Ao iluminar o link, posicionado o mouse sobre ele, muitas vezes é possível ver o endereço real da página falsa ou código malicioso;

• Utilize mecanismos de segurança, como programas antimalware, firewall pessoal e filtros antiphishing;

• Analise se a página utiliza conexão segura. Sites de comércio eletrônico ou Internet Banking confiáveis sempre utilizam conexões seguras quando dados sensíveis são solicitados;

• Investigue as informações mostradas no certificado. Caso a página falsa utilize conexão segura, um novo certificado será apresentado e, possivelmente, o endereço mostrado no navegador Web será diferente do endereço correspondente ao site verdadeiro;

• Acesse a página da instituição que supostamente enviou a mensagem e procure por mais informações. Você vai observar que não faz parte da política da maioria das empresas o envio de mensagens, de forma indiscriminada, para seus usuários;

• Erros de português ainda são muito comuns no phishing. Leia as mensagens recebidas com atenção e não clique em nada ao identificar problemas no texto;

• Duvide das mensagens impessoais, do tipo: “Caro cliente”.

Smishing

O que é?

- Tipo de phishing que envolve uma mensagem de texto. Na maioria das vezes, via SMS.
- As mensagens normalmente contêm algum tipo de urgência, para tentar fazer o destinatário agir imediatamente.

Mas como?

- O cibercriminoso se passa por uma empresa séria;
- Envia um link de site falso, onde as informações fornecidas serão usadas para cometer roubo de identidade, fraude e outros crimes.

Quero exemplos!

- Você recebe uma mensagem de texto de um suposto varejista;
- Ele pede para você verificar suas informações de faturamento ou diz que "seu pacote não será enviado a tempo";

- Você abre o link, cede os dados e...

Pronto!

Eles serão usados para:

- Cometer roubo de identidade, fraudes e outros crimes;
- E os criminosos poderão distribuir malwares e spywares para realizar outras tarefas maliciosas.

Vishing

O que é?

- Variação de phishing por meio de ligação telefônica ou mensagens de voz.
- Pode ocorrer via robocalls pré-gravados ou pela tática do falso atendente de uma empresa legítima.

Quase sempre começa no ponto em que o phishing e o smishing terminam. Exemplo:

- Você acessa uma plataforma de mídias sociais;
- Clica em um link tentador;
- Aparece uma tela avisando que deve ligar para um número "x" para reparar um erro grave no computador;
- Um técnico solícito atende o telefone, disposto a ajudar mediante a cobrança de uma taxa;
- Você passa as informações do seu cartão de crédito ou transfere o valor para pagar pelo "software" que "resolverá seu problema";
- O técnico "atencioso" desaparece, ninguém mais atende o telefone e o seu problema não é solucionado.

Como isso aconteceu?

O malware incorporado ao link acionou um bloqueio que somente o "técnico" seria capaz de corrigir.
Tudo isso, claro, porque foi a própria "empresa" dele que gerou o problema.
Atenção: esses links também podem aparecer em anúncios on-line direcionados aos consumidores.

"Sim ou não" por quê?

Desconfie de gravações que recebe sem solicitar pedindo que você responda "sim ou não".
Golpistas podem gravar sua voz e fazer uma pergunta que exija um "sim".
Essa gravação pode ser usada para fingir ser você ao telefone e autorizar cobranças ou acesso às suas contas.

Mais prevenção!

- Pergunte pelo nome, cargo e empresa de quem te ligou;
- Mesmo que forneçam essas informações, verifique sua legitimidade: ligue para um número de telefone oficial público da organização.

Respire

É fácil ser enganado sob pressão em situações de urgência!
Anote qualquer informação que a pessoa forneça durante a chamada, sem fornecer seus dados pessoais.

Não retorne ligações desconhecidas

Ao receber chamadas não solicitadas de qualquer pessoa oferecendo serviços, não retorne de seu próprio celular/telefone.
Existe uma tecnologia que bloqueia a linha telefônica da vítima depois que a chamada é encerrada e redireciona suas próximas ligações para a origem fraudulenta.

#FicaAdica:

Prefira **VOCÊ** buscar um telefone público da eventual empresa para saber mais sobre o produto/serviço.

Sentiu que é armadilha?

• Denuncie mensagens, anúncios e perfis maliciosos, usando as opções disponibilizadas pelas plataformas;

• Bloqueie números de telefone e contas que enviam mensagens maliciosas sempre.

FUI VÍTIMA. E agora?

Monitore sua vida financeira e sua identidade!

O furto da sua identidade pode causar muitos prejuízos. Você pode ficar com dívidas em seu nome, perder reputação e crédito e ainda se envolver em processos judiciais;

• Ative alertas e monitore extratos de cartões e contas bancárias;

• Contate as instituições envolvidas para esclarecer dúvidas ou contestar irregularidades;

• Acompanhe seus registros financeiros junto ao Banco Central;

Registre ocorrência junto à autoridade policial, caso:

• Alguém esteja se passando por você (furto de identidade);

• Se tiver prejuízos financeiros.

Sinais de furto de identidade:

notificações de instituições de proteção ao crédito, contas bancárias, empréstimos, cartões ou benefícios que não solicitou.

Referências

Safernet

https://new.safernet.org.br/

Cert

https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf

Kaspersky

https://www.kaspersky.com.br/blog/

UFBA

https://gsic.ufba.br/sites/gsic.ufba.br/files/ciberseguranca-como-ser-vitima-nem-vilao.pdf

Tribunal de Justiça do Distrito Federal e dos Territórios

https://www.tjdft.jus.br/publicacoes/edicoes/manuais-e-cartilhas/cartilha_segurancavirtual_22abr2021.pdf