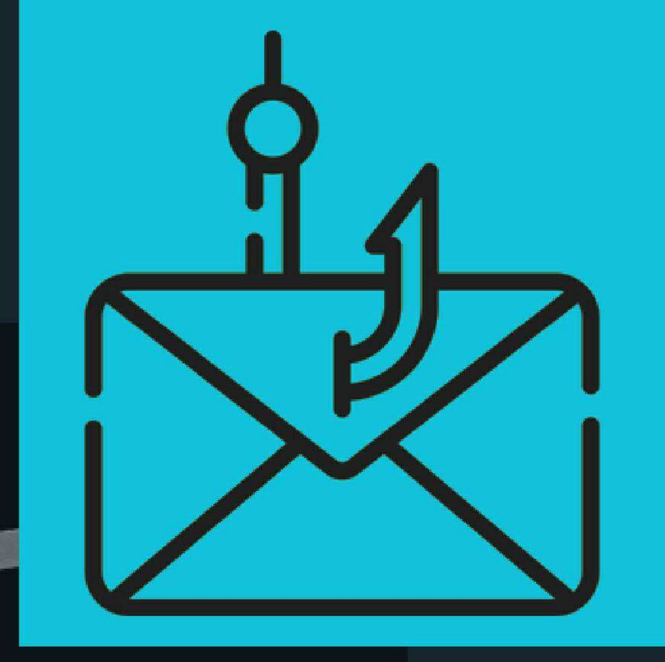


O PERIGO DO PHISHING

SINDPASS

PROTEGENDO-SE CONTRA AMEAÇAS CIBERNÉTICAS

O Perigo do Phishing

Protegendo-se contra Ameaças Cibernéticas

No mundo digital atual, onde a tecnologia desempenha um papel fundamental em nossas vidas, é essencial estarmos cientes dos perigos que espreitam nas profundezas da Internet. Uma das ameaças mais comuns e sofisticadas que os usuários enfrentam é conhecida como *phishing*.

O *phishing* é uma prática cibernética maliciosa na qual os criminosos se passam por entidades confiáveis, como bancos, empresas de comércio eletrônico e provedores de serviços, para obter informações pessoais e confidenciais dos usuários. Eles utilizam métodos engenhosos para manipular e enganar as pessoas, induzindo-as a revelar detalhes como senhas, números de cartões de crédito e informações de identificação.

O objetivo principal dos golpistas é obter acesso a dados sensíveis para cometer fraude financeira, roubo de identidade e até mesmo acessar sistemas corporativos. Eles se aproveitam da confiança e ingenuidade das pessoas, explorando técnicas psicológicas e táticas persuasivas para induzi-las a compartilhar informações valiosas.

Explorando os tipos de phishing

Por e-mail

O phishing por e-mail é uma das formas mais comuns e conhecidas de ataque. Os criminosos enviam e-mails falsos que se passam por comunicações legítimas de empresas confiáveis, como bancos, instituições governamentais ou provedores de serviços. Esses e-mails costumam conter links maliciosos que direcionam as vítimas para sites fraudulentos, onde são solicitadas informações pessoais e confidenciais, como senhas, números de cartão de crédito ou informações bancárias. Os e-mails de phishing também podem conter anexos maliciosos que, quando abertos, infectam o computador da vítima com malware.

Smishing (por SMS)

Com o aumento do uso de dispositivos móveis, os criminosos também adaptaram suas táticas de phishing para aproveitar essa tendência. O smishing envolve o envio de mensagens de texto falsas que se passam por organizações legítimas, como bancos, empresas de entrega ou serviços de telefonia móvel. Essas mensagens de texto geralmente solicitam às vítimas que cliquem em links ou respondam com informações pessoais. O objetivo é enganar as pessoas e levá-las a compartilhar dados sensíveis através de mensagens de texto.

Explorando os tipos de phishing

Vishing (por Voz)

O vishing, também conhecido como phishing por voz, é uma forma de ataque em que os criminosos utilizam chamadas telefônicas para enganar as vítimas. Eles se passam por representantes de instituições financeiras, empresas de telecomunicações ou até mesmo agências governamentais, e solicitam informações pessoais e confidenciais. Os golpistas podem usar técnicas de engenharia social, como manipulação emocional ou criação de senso de urgência, para convencer as vítimas a fornecerem dados sigilosos.

Whisker Phishing

O whisker phishing é uma forma de ataque mais direcionada que envolve a coleta de informações pessoais de uma pessoa para criar uma persona falsa e, assim, estabelecer uma conexão confiável com a vítima. Os criminosos podem vasculhar as redes sociais, fóruns online ou outras fontes para obter informações como hobbies, interesses ou conexões pessoais. Essas informações são usadas para criar uma abordagem personalizada que visa enganar a vítima de forma mais eficaz.

Como identificar um ataque

SINAIS QUE INDICAM O PHISHING

Verifique o remetente do e-mail

Um dos primeiros passos para identificar um ataque de phishing é verificar o remetente do e-mail. Os criminosos costumam usar endereços de e-mail falsos ou semelhantes aos de empresas legítimas para enganar as vítimas. Verifique cuidadosamente o endereço de e-mail do remetente para identificar possíveis discrepâncias ou erros ortográficos.

Analise o conteúdo do e-mail

Leia o conteúdo do e-mail com atenção. Os e-mails de phishing geralmente contêm erros ortográficos, gramaticais ou de formatação. Fique atento a mensagens que pareçam urgentes, ameaçadoras ou que solicitem informações pessoais e confidenciais. Empresas legítimas raramente solicitam informações confidenciais por e-mail.

SINAIS QUE INDICAM O PHISHING

Como identificar um ataque

Desconfie de links e anexos suspeitos

Links maliciosos e anexos são componentes comuns de ataques de phishing. Evite clicar em links suspeitos presentes em e-mails, mensagens ou sites não confiáveis. Passe o cursor do mouse sobre o link (sem clicar) para visualizar o destino real do link. Além disso, desconfie de anexos não esperados ou de formatos desconhecidos, pois podem conter malware.

Observe solicitações incomuns

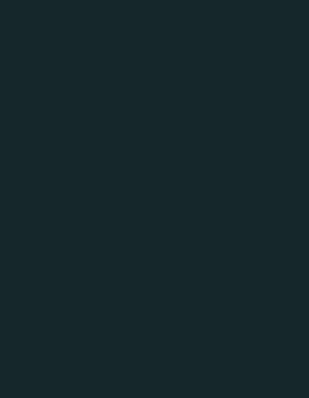
Os ataques de phishing frequentemente solicitam informações pessoais ou financeiras. Desconfie de solicitações incomuns, como fornecer senhas, números de cartão de crédito, números de segurança social ou outras informações confidenciais. Empresas legítimas geralmente não solicitam essas informações por e-mail.

Como identificar um ataque

SINAIS QUE INDICAM O PHISHING

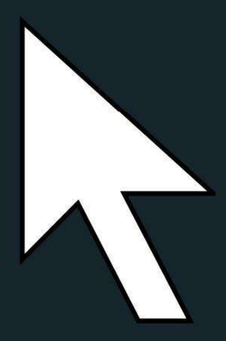
Preste atenção a mensagens de texto suspeitas

O phishing também pode ocorrer por meio de mensagens de texto, conhecido como smishing. Fique atento a mensagens de texto que solicitam informações pessoais ou que contenham links suspeitos. Não clique em links ou forneça informações confidenciais por mensagem de texto, a menos que você tenha verificado a autenticidade da fonte.



Verifique a autenticidade de sites

Ao receber um e-mail que solicita que você clique em um link e faça login em um site, verifique a autenticidade do site antes de inserir suas informações de login. Observe a URL do site para verificar se há discrepâncias ou erros ortográficos. Procure por um cadeado na barra de endereços e certifique-se de que a conexão seja segura (https://)



Proteja-se

Usar estratégias eficazes ajudam a evitar cair em armadilhas cibernéticas

1

Fique atento a sinais de alerta que podem indicar um ataque de phishing. Erros ortográficos, gramaticais ou de formatação nos e-mails podem ser indícios de que algo não está certo. Verifique se o remetente é legítimo e se o e-mail contém solicitações incomuns ou urgentes para fornecer informações pessoais ou financeiras.

2

Evite clicar em links presentes em e-mails, mensagens de texto ou mensagens instantâneas que pareçam suspeitos. Os criminosos podem direcioná-lo para sites falsos que se parecem com os legítimos, mas são projetados para roubar suas informações. Em vez disso, digite manualmente o endereço do site no seu navegador ou entre em contato diretamente com a empresa para verificar a autenticidade do pedido.

Proteja-se

3

Anexos em e-mails podem conter malware ou vírus que podem comprometer a segurança do seu dispositivo. Certifique-se de que o anexo seja de uma fonte confiável e, mesmo assim, escaneie-o com um antivírus atualizado antes de abri-lo. Se você não estiver esperando um anexo ou se parecer suspeito, é melhor não abrir.

4

Use senhas fortes e únicas para suas contas online. Evite senhas óbvias, como datas de nascimento ou sequências numéricas simples. É recomendável usar uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais. Além disso, não compartilhe suas senhas com ninguém e evite reutilizá-las em diferentes plataformas.

Proteja-se

5

Empresas legítimas nunca solicitam informações pessoais, como senhas, números de cartão de crédito ou números de segurança social, por e-mail ou mensagem. Nunca compartilhe essas informações confidenciais em resposta a solicitações não solicitadas. Entre em contato diretamente com a empresa por meio de canais confiáveis para verificar se a solicitação é legítima.

6

Mantenha seu sistema operacional, navegadores da web e aplicativos atualizados com as versões mais recentes. As atualizações de software geralmente incluem correções de segurança importantes que protegem contra vulnerabilidades exploradas pelos golpistas. Ativar atualizações automáticas é uma maneira eficaz de garantir que você esteja sempre protegido.

Este e-book foi desenvolvido pelo Sindpass
em conjunto com o escritório Cotrim Advogados
e LP Consultoria e é parte integrante do material
apresentado na adequação à LGPD.

SINDPASS