Guia de Prevenção contra golpes

CARTILHA:

SICOOB Carlos Chagas

SUMÁRIO

SICOOB
Carlos Chagas

Engenharia Social

O que é?

É uma técnica empregada por golpistas para induzir usuários desavisados a repassarem dados confidenciais (ex: senhas e dados de cartões de crédito), infectar seus terminais com malwares (vírus) ou abrir links parasitas infectados.

Ao contrário do que muitos pensam, não é necessário nenhum equipamento de tecnologia avançada para realizar essa atividade. Na verdade, a engenharia social é simplesmente uma manipulação psicológica do usuário, de modo a convencê-lo a fazer o que o criminoso quer, burlando procedimentos básicos de segurança.

A Engenharia Social é um golpe antigo que se manifesta em todas as áreas da vida. Por isso seria um erro pensar que é algo novo, ou que você só detecta no mundo on-line.

De fato, a Engenharia Social tem sido usada no mundo físico há muito tempo. Existem inúmeros exemplos de criminosos que se apresentam como chefes de bombeiros, técnicos, exterminadores e zeladores, com o único objetivo de entrar no prédio de uma empresa e roubar segredos corporativos ou dinheiro.

Golpes com Cartões

Como acontece?

Falso motoboy

Se você receber uma ligação dizendo que há transações suspeitas em seu cartão e que será enviado um motoboy para coletá-lo, não passe informações (especialmente sua senha) e desligue na hora.

*Lembre-se de que nenhuma instituição financeira tem essa prática.

No comércio

O golpista fica de olho na senha digitada pela pessoa e, após a vitima usar a maquininha, devolve um cartão parecido de outra pessoa. Eles também usam de alguma distração para pedir que a pessoa digite a senha no campo de valor.

No caixa eletrônico

O golpista oferece ajuda para usar o terminal de atendimento, guardando a senha, e trocando o cartão da vítima por outro muito parecido.

SICOOB
Carlos Chagas

Golpes com falsos funcionários

Como atuam?

Golpistas entram em contato, se passando por funcionários da instituição financeira para obter informações confidenciais. Embora o repertório de contato tenha inúmeras variações, por vezes mencionam inclusive que trabalham na área de segurança e que precisam confirmar supostas transações realizadas.
A intenção dos golpistas é coletar informações pessoais e dados bancários para utilização indevida.

FIQUE ATENTO

- Nunca forneça essas informações por telefone, ou através de links recebidos por SMS, WhatsApp, e-mails, redes sociais, entre outros.

- Não digite seus dados em uma suposta central de atendimento.

- Nesse tipo de golpe, os golpistas podem até simular o número de telefone da instituição financeira e usar recursos tecnológicos, como gravações e menus para aumentar a sua confiança.

Independente do motivo do contato, nunca pediremos:

- **Suas senhas;**
- **Código token;**
- **Códigos recebidos por SMS.**

Golpe por WhatsApp

Como acontece?

Nesse golpe, o WhatsApp da vítima é clonado por golpistas que fingem ser do serviço de atendimento de sites de compra para roubar a conta no aplicativo. Com a conta disponível os golpistas enviam mensagens pelo aplicativo se fazendo passar pela pessoa e solicitam dinheiro emprestado aos seus contatos mais conhecidos

Como evitar:

A medida mais simples e eficaz para evitar que o WhatsApp seja clonado **é habilitar a opção "Verificação em duas etapas" (Configurações/Ajustes > Conta >Verificação em duas etapas).** Dessa forma, é possível cadastrar uma senha que será solicitada periodicamente pelo aplicativo.

DICA DE PRIVACIDADE:

E, para evitar que sua foto seja utilizada indevidamente, você pode exibi-La apenas para seus contatos de confiança. Esse cuidado vai evitar que golpistas usem a sua imagem e se passem por você para enganar seus conhecidos.
É simples ativar essa opção:

IOS: no WhatsApp, acesse Ajustes> Conta> Privacidade > Foto de perfil> Meus contatos
ANDROID: no WhatsApp, acesse Menu> Configurações > Conta > Privacidade> Foto de perfil> Meus contatos

SICOOB
Carlos Chagas

Phishing

O que é?

Phishing é um termo originado do inglês (fishing), que em computação se trata de um tipo de roubo de identidade online. Essa ação fraudulenta é caracterizada por tentativas de adquirir ilicitamente dados pessoais de outra pessoa, sejam senhas, dados financeiros, dados bancários, números de cartões de crédito, ou simplesmente dados pessoais.
Os golpistas enviam milhões de mensagens por dia, na esperança de encontrar vários usuários inexperientes que possam ser vítimas do ataque.

GOLPES MAIS COMUNS:

Golpe do bloqueio de conta
O golpista envia um falso e-mail ou SMS sobre bloqueio de conta em nome da instituição financeira informando possíveis irregularidades em seu cadastro, ou pedindo uma atualização dessas informações, que pode levar ao bloqueio total da conta.

Golpe da atualização cadastral ou atualização de segurança
O golpista envia um e-mail ou SMS com link em nome da instituição financeira, informando a falta de atualização ou sincronização do código, pedindo senhas e informações pessoais. A vítima é direcionada para um formulário ou página falsa, que captura os dados da vítima para o golpista usar posteriormente.

Sites falsos

O que são sites falsos?

Com a internet, muitos comportamentos mudaram. Hoje realizamos muitas de nossas compras on-line, mas ainda não nos acostumamos a conferir a veracidade desses sites e os requisitos básicos de segurança para garantir que estamos em um ambiente seguro.
Assim, golpes envolvendo sites falsos são bastante recorrentes e costumam iniciar pelo envio de links por SMS, e-mails e anúncios em redes sociais.
O objetivo é atingir clientes de sites de comércio eletrônico através de um site quase idêntico ao verdadeiro. As vítimas não percebem a fraude, escolhem os produtos desejados e realizam o pagamento sem saber que nunca vão receber a mercadoria.

DICAS PARA NÃO CAIR NESSE GOLPE

- **Faça uma pesquisa de mercado comparando preços**. Desconfie se o valor for muito baixo.
- **Confira de forma minuciosa,** o endereço **(URL)** do site em que está comprando. Sites falsos possuem domínios bastante similares aos verdadeiros.

-Dê preferência a sites cujos domínios terminem **.com.br.** Sites que possuem domínios **.com** normalmente indicam que estão hospedados em servidores situados fora do Brasil
– Não clicando em links que direcionem direto aos sites de compras. Esses sites podem ser falsos e conter malware **(vírus),** capaz de copiar dados sigilosos.

SICOOB
Carlos Chagas

Boleto falso

Como identificar?

Boletos falsos possuem um formato bastante semelhante ao dos boletos originais, mas apresentam algumas diferenças que apontam que os dados possam ter sido manipulados, principalmente em relação à linha digitável na qual constam os dados da conta bancária que receberá o valor a ser pago. Com a adulteração da linha digitável, os golpistas conseguem fazer com que o dinheiro da vítima vá para contas bancárias dos próprios golpistas ou de "laranjas"

Confira:

I. O nome e a logomarca do banco emissor devem ser coincidentes;

II. o número do banco deve corresponder ao banco contido na logomarca e no campo nome do banco. Em caso de dúvida acesse http:J /www.buscabanco.org.br.

III. Os três primeiros caracteres da linha ditável devem ser iguais ao número do banco e correspondente.

Os números contidos nos campos: Agência, Código cedente e nosso número devem de alguma forma estar contidos na linha digitável, independente do banco emitente do boleto, e da localização destas informações na linha digitável.

Cuidados com o Pix

Fique atento

- Cadastro da sua chave Pix deve ser realizado somente no ambiente seguro da sua instituição financeira, através do Internet Banking ou Mobile Banking. Os aplicativos móveis devem ser instalados a partir das lojas oficiais da Apple (Apple Store) e do Google (Play Store).

- Cuidado com e-mails ou mensagens de WhatsApp sobre convites de pré-cadastro ou cadastro do Pix. Na dúvida, não passe nenhuma informação.

- Cuidado com ligações de "supostos funcionários" da sua instituição financeira oferecendo o cadastramento do Pix, ou mesmo oferecendo um serviço de atualização via conexão remota com o argumento de atualizar ou fazer um teste. Na dúvida, desligue e entre em contato com seu Gerente.

- Não faça transferências ou realize transações para supostamente fazer um teste na sua chave Pix - isso não existe!

Sempre confira os dados do "recebedor" da transação Pix (pagamento ou transferência), seja para uma pessoa ou um estabelecimento.

SICOOB Carlos Chagas

Senhas e autenticações

O que é?

As senhas permitem a autenticação do usuário quando do acesso a suas contas nas mais diversas plataformas e dispositivos eletrônicos no melo corporativo, garantindo que apenas pessoas autorizadas tenham acesso a determinados equipamentos e informações, validando a identidade e autenticando o usuário para assegurar sua legitimidade de acesso.
Diante da relevância da utilização adequada das senhas para a proteção de informações, é fundamental a escolha e utilização de senhas seguras em suas contas e dispositivos eletrônicos, sendo recomendável a atuação das empresas no sentido de exigí-las em todas as ferramentas corporativas.

Como criar uma senha de segura?

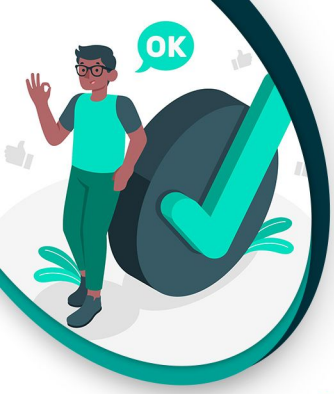
- As senhas devem ser compostas por, no mínimo, 8(oito) caracteres;

- Suas senhas devem ser alteradas com frequência e nunca devem ser repetidas senhas utilizadas anteriormente;

- Fiquem atentos a informações sobre vazamento de dados de determinados serviços. Se houver esse tipo de ocorrência, em um serviço utilizado, modifiquem as credenciais de acesso, para evitar que dados sejam obtidos por terceiros

- Não utilizem apenas letras ou números. Senhas seguras devem conter letras maiúsculas e minúsculas, números e caracteres não alfanuméricos (tais como@. $.#etc.);

- Não componham suas senhas com seus nomes e/ou sobrenomes, nome da empresa em que trabalham ou qualquer variação desse tipo.



CONTATOS OFICIAIS

E-mail corporativo

sicoobcarloschagas@sicoobcarloschagas.com.br

Site

www.sicoobcarloschagas.com.br

Redes sociais

@sicoobcarloschagas
@sicoobcarloschagas

SICOOB
Carlos Chagas

ONDE ESTAMOS?

NOSSAS AGÊNCIAS

Matriz - Carlos Chagas
Av. Capitão João Pinto, 17-B - Centro
Fone: (33) 3624-1258

Pavão
Rua Getúlio Vargas, 113 - Centro
Fone: (33) 3535-1237

Águas Formosas
Rua José Quaresma da Costa, 200 - Centro
Fone: (33) 3611-1100

Machacalis
Rua Salvador, 71 - Centro
Fone: (33) 3627-1210

Santa Helena de Minas
Rua Belo Horizonte, 131 - Centro
Fone: (33) 3626-9233

Bertópolis
Rua Governador Valadares, 355 - Centro
Fone: (33) 3626-1414

Teixeira de Freitas
Av. Presidente Getúlio Vargas, 2219-B - Bela Vista
Fone: (73) 3263-5324

Dicas rápidas

Para manter seu computador seguro

- Instale um bom programa de antivírus e, pelo menos uma vez por semana, faça uma verificação completa do computador;
- Use sempre cópia original do programa de antivírus, pois as cópias *piratas* geralmente já estão infectadas e não funcionam corretamente;

Fique atento aos endereços acessados no seu navegador

-Verifique se o endereço que está aparecendo em seu navegador é realmente o que você deseja acessar;
- Não confie em tudo o que vê ou lê;

Compras e Pagamentos

-Ao realizar compras pela Internet procure por sites reconhecidamente seguros;
-Se for utilizar o seu cartão de crédito ou tiver que fornecer dados bancários, verifique se a página acessada utiliza tecnologia de criptografia;
- Opte por usar o cartão virtual para compras online;

Troque suas senhas com certa frequência

- É uma boa prática trocar sua senha periodicamente para reduzir a possibilidade de que alguém venha a sabê-la e possa usá-la no futuro.

- Nunca abra e-mails ou execute arquivos enviados por desconhecidos

SICOOB
Carlos Chagas

Sicoob online

App´s oficiais

App Sicoob
Gerencie a sua vida financeira pelo app sem precisar sair de casa.

App Sicoobcard
Controle suas compras e acompanhe suas faturas no momento que você quiser.

App Sipag
Administre suas vendas e visualize seus rendimentos direto do seu celular, de onde estiver, quando quiser.

App Sicoob Moob
Fique por dentro de tudo o que acontece na sua cooperativa, de onde você estiver.

www.sicoobcarloschagas.com.br

GUIA DE PREVENÇÃO CONTRA Ggolpes

QR CODE

LEIA O QR CODE
E SAIBA MAIS!

SICOOB
Carlos Chagas