CAMPANHA DE PREVENÇÃO E COMBATE A FRAUDE

VERDADEIRO OU FRAUDE

Setor de Controles e Riscos

SICOOB Centro-Sul Mineiro

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 para sites infectados.

Ao contrário do que muitos pensam, não é necessário qualquer 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 o vê 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 receber uma ligação dizendo que há transações supeitas 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
0 golpista fica de olho na senha digitada pela pessoa e, após a vítima usar a maquininha, devolve um cartäo parecido de outra pessoa. Eles também usam de alguma distraçäo para pedir que a pessoa digite a senha no campo de valor.

No caixa eletrônico
0 golpista oferece ajuda para usar o terminal de atendimento, guardando a senha e trocando o cartäo da vítima por outro muito parecido.

Gerencie o seu cartão por meio do aplicativo Sicoobcard:

Matenha bloqueado as compras online e só desbloquei quando for efetuar compras pela internet, ou a contratação por aplicativos como por exemplo Uber e Ifood

Utlize o cartão virtual único, que você poderá gerar pelo próprio aplicativo sicoobcardad ou sicoobnet celular. Dessa forma o cartão poderá ser utilizado apenas uma vez, e mesmo que haja vazamento dos dados cadastrados no site de compra, nenhuma outra pessoa conseguirá usar o cartão novamente.

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.
Também podem oferecer uma falsa quitação de empréstimo. Nesse tipo de golpe, o golpista se passa por funcionário da instituição financeira e oferece ao associado descontos significativos para quitação dos débitos.

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.**

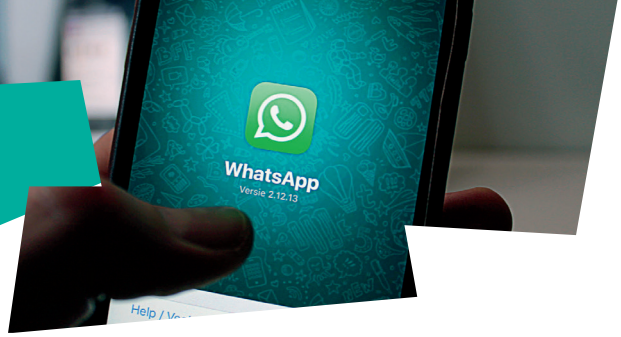
Independente do motivo do contato, nunca pediremos:

•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

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 dele, que pode levar a conta ao bloqueio total.

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 OS SITES FALSOS?

Com a internet, muitos comportamentos mudaram. Hoje realizamos muitas de nossas compras online, mas ainda não 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 como instagram e facebook.

O objetivo é atingir clientes de sites de comércio eletrônico através de um site quase idêntico ao verdadeiro, sendo exemplo os sites de grandes lojas de varejo e também sites de leilões. As vítimas não percebem a fraude, escolhem os produtos desejados e realizam o pagamento sem saber que nunca vão receber a mercadoria. Também tem ocorrido o anúncio de vendas de eletrodomésticos e móveis no instagram e facebook hackeados, onde o comprador acha que está negociando com uma pessoa conhecida, quando na verdade não é.

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 terminam em .com.br. Pois 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

BOLETO FALSO

COMO IDENTIFICAR?

Boletos falsos possuem um formato bastante semelhante ao dos boletos originais, mas apresentam algumas diferenças que apontam terem sido os dados 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 vitima vá para contas bancárias dos próprios golpistas ou de"laranjas".

Confira:

- O nome e a logomarca do banco emissor devem ser coincidentes;
- O número do banco deve corresponder ao banco contido no logotipo e no campo nome do banco. Em caso de dúvida acesse *http://www.buscabanco.org.br*

- Os três primeiros caracteres da linha digitável devem ser iguais ao número do banco e correspondente ao nome do banco e seu logotipo.

- 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.

- Evite atualizar boletos vencidos via internet. Caso seja necessário ligue no número que você tem certeza que é do fornecedor e solicite um boleto atualizado.

- Na hora de confirmar o pagamento no aplicativo do Sicoob ou Caixa Eletrônico, verifique se os dados do beneficiário são os mesmos dados contidos no boleto, e se realmente o nome apresentado na tela de confirmação é da pessoa ou empresa que você contratou algum serviço ou efetuou a compra de mercadorias. Se houver divergência não confirme o pagamento entre em contato com fornecedor pelos contatos oficiais.

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 os e-mails ou mensagens de WhatsApp sobre convite 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!

Antes de fazer qualquer transferência via pix, certifique-se que está enviado o valor para o pessoa correta, pois como o PIX é instantâneo, caso seja fraude, dificilmente você conseguirá a devolução do valor. Uma vez que assim que os criminosos rebem os créditos em suas contas, já transferem para outras.

FALSA VENDA DE GADO E VEÍCULOS

COMO ACONTECE?

O fraudador aparece como intermediador do compra e da venda de produtos anunciados na internet. Geralmente cria uma falsa história que o vendedor possui um dívida com ele. Pede para que o comprador não combine valores com o vendedor e solicita a transferência financeira para uma conta distinta da conta do vendedor.

DICAS PARA NÃO CAIR NESSE GOLPE

Antes de efetuar qualquer transferência financeira certifique-se que realmente está transferido o dinheiro para o vendedor legítimo. Jamais faça a transferência se na operação estiver envolvido a conta de terceiros estranhos a operação.

SENHAS E AUTENTICAÇÕES

O QUE É?

As senhas permitem a autenticação do usuário quando do acesso às suas contas nas mais diversas plataformas e dispositivos eletrônicos no meio 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 proteçao 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 exigi-las em todas as ferramentas corporativas.

Como criar uma senha segura?

- As senhas devem ser compostas por, no mínimo, 8(oito) caracteres;
- Não utilizem apenas letras ou números; Senhas seguras devem conter letras maiúsculas e minúsculas, números e caracteres não alfanuméricos (tais como @, frequência e nunca devem ser repetidas $,# etc.);
- Suas senhas devem ser alteradas com frequência e nunca devem ser repetidas senhas utilizadas anteriormente;
- Não componham suas senhas com seus nomes e/ou sobrenomes, nome da empresa ou qualquer variação desse tipo.
- Fiquem atentos a informações sobre vazamento de dados de serviços. Se houver esse tipo de ocorrência; em um serviço atualizado, modifiquem as credenciais de acesso, para evitar que dados sejam obtidos por terceiros.

CONTATOS OFICIAIS SICOOB CENTRO-SUL MINEIRO

SICOOB
Centro-Sul Mineiro

Sicoob Centro-Sul Mineiro

www.sicoob.com.br/web/sicoobcentrosulmineiro/

NOSSAS AGÊNCIAS

· Matriz - Carmópolis de Minas
Rua Luís Alves, 134 - Centro
Carmópolis de Minas - MG - CEP: 35534-000
contato@sicoobcentrosulmineiro.com.br

37 33331522 37 999388343 11:00-15:00h

· Andrelândia
Rua Dr. Ernesto Braga, 11 - Centro
Andrelândia - MG - CEP: 37300-000
contato@sicoobcentrosulmineiro.com.br

35 33251331 35 991038936 11:00-15:00h

· Carrancas
Praça Manoel Moreira, 398 - Centro
Carrancas - MG - CEP: 37245-000
contato@sicoobcentrosulmineiro.com.br

35 33271752 10:00-14:00h

· Carvalhos
Praça Ana Dantas Motta, 38 - Centro
Carvalhos - MG - CEP: 37456-000
contato@sicoobcentrosulmineiro.com.br

35 33451172 11:00-15:00h

· Cruzília
Rua Coronel Maciel, 27 - Centro
Cruzília - MG - CEP: 37445-000
contato@sicoobcentrosulmineiro.com.br

35 33461994 11:00-15:00h

· Itaguara
Praça Raimundo de Morais Lara, 32 - Centro
Itaguara - MG - CEP: 35488-000
contato@sicoobcentrosulmineiro.com.br

31 31842550 37 9 99588189 11:00-15:00h

· Minduri
Avenida Getúlio Vargas, 152 - Centro
Minduri - MG - CEP: 37447-000
contato@sicoobcentrosulmineiro.com.br

35 33261388 35 999357836 10:00-14:00h

· Passa Tempo
Praça Raul Leite, 160 - Centro
Passa Tempo - MG - CEP: 35537-000
contato@sicoobcentrosulmineiro.com.br

37 33351162 37 998335609 11:00-15:00h

· Piracema
Rua Ouro Preto, 285 - Centro
Piracema - MG - CEP: 35536-000
contato@sicoobcentrosulmineiro.com.br

37 33341224 11:00-15:00h

· São Vicente de Minas
Rua Marechal Floriano Peixoto, 265 - Centro
São Vicente de Minas - MG - CEP: 37370-000
contato@sicoobcentrosulmineiro.com.br

35 33231529 35 991252567 11:00-15:00h

· Seritinga
Praça Sete de Setembro, 335 - Centro
Seritinga - MG - CEP: 37454-000
contato@sicoobcentrosulmineiro.com.br

35 33231529 11:00-15:00h

· PA de Negócios
Rua Francisco Paolinelli, 155 - Centro
Carmópolis de Minas - MG - CEP: 35534-000
contato@sicoobcentrosulmineiro.com.br

37 33331522 08:00-17:00h

DICAS RÁPIDAS

Para manter seu computador seguro

- lnstale um bom programa de antivirus 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;

- Náo 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 cartáo de crédito ou tiver que fornecer dados bancarios, verifique se a página acessada utiliza tecnologia de criptografia:

- Opte por usar o cartao virtual para compras online;

Troque suas senhas com certa frequência

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

Nunca abra e-mails ou execute arquivos enviados por desconhecidos

QUER MAIS DICAS?

ACESSE NOSSAS REDES SOCIAIS E SAIBA MAIS...

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.