Autoria: Silvio Ferreira

Finalidade: educativa e comunitária (Extensão UniCV)

Essencial saber

Este capítulo é de extrema importância (na verdade todos são), pois, agora você vai estudar os principais golpes, os mais conhecidos. Neste exato momento, pessoas estão caindo em algum desses golpes ou em golpes muito semelhantes.

Não abordei todos. Isso porque novos golpes surgem a todo momento. De acordo com a Serasa Experian, a cada oito segundos, um brasileiro sofre uma tentativa de fraude.

Mas, sem dúvida alguma, através do estudo de cada tópico a seguir você ficará muito mais preparado.

O estudo constante é uma das bases da segurança. Estudar e conhecer alguns tipos de ameaças que podemos enfrentar ao usar a internet é essencial. Somente dessa forma você ficará atento e preparado para se proteger.

Phishing

O primeiro golpe, fraude, falcatrua, farsa, tapeação, que explico para você é justamente o mais corriqueiro na internet. O Próprio Google possui mecanismos para identificar sites que são fontes ou apresentam algum risco deste tipo: o "famoso" phishing.

Primeiro vamos entender o significado dessa palavra. Phishing é uma palavra derivada de fishing. E fishing é traduzida literalmente como pescaria.

Mas o que tem a ver phishing com pescaria? Calma que você vai entender facilmente.

Imagine que toda a internet é o aceano. Quando eu digo toda a internet, me refiro a todos os serviços possíveis: web (para navegar em websites), e-mails, aplicativos de comunicação instantânea, e tudo mais. Não sei se você tem esse conhecimento, mas a internet engloba muitos serviços e a web (por exemplo) é só um deles. É através da web que usamos os sites (websites). Se você não possui

esse conhecimento, este livro não é o lugar para buscá-lo. Sugiro que procure aprender sobre isso (internet básica).

Vamos continuar: o fraudador é o pescador. E ele joga no oceano da internet uma ou mais iscas (ou várias) para pegar os peixes. Quem são os peixes? Eu, você e todos todos nós. Obviamente, após a leitura deste livro, você NÃO será mais um peixe fácil de pegar.

Quando os peixeis são pegos pelas iscas, o fraudador roubará dados pessoais deles, que pode ser, por exemplo, todos os dados do cartão de crédito: nome impresso no cartão, número do cartão, código de segurança e até senha. E como isso é possível? Ora, o próprio peixe, que é muito inocente, digitou tudinho em uma página falsa.

Quando eu digo "página falsa" ou "site falsificado" estou me referindo a um site/página que geralmente é um clone de algum site/página oficial. Um site ou página falsa levará o usuário ao engano, fazendo-o pensar que está em um ambiente oficial e seguro.

A partir daí a dor de cabeça será tremenda. Se o peixe descobrir a tempo ele poderá providenciar o bloqueio do cartão. Caso contrário, ele perceberá a fraude somente quando começar a surgir várias compras que ela não fez em seu extrato. E a dor de cabeça será igualmente inevitável. Terá que ligar para a operadora/banco do cartão, tentar pedir o cancelamento da compra, bloquear o cartão e etc, etc, etc ...

O phishing propriamente dito é isso que acabei de explicar. É um golpe através da internet cujo objetivo é capturar informações pessoais de uma pessoa, de uma vítima, de um peixe.

Esses dados pessoais podem ser dados de cartões (como acabei de mencionar), ou qualquer outro dado pessoal, como nome de usuário e senha para acessar algum tipo de sistema, CPF, endereço, dados de empresa, número de telefone e tudo mais que o fraudador estiver buscando.

Agora vamos entender a mecânica da coisa, como tudo funciona. O phishing é um recurso que vem da engenharia social (que foi abordada no capítulo anterior).

Apenas para recapitular (eu sei que é chato, mas, preciso dessa informação agora): a engenharia social possui **técnicas**, e a maioria dessas técnicas se resumem em obter informações pessoais ou privilegiadas da vítima. E para conseguir isso o fraudador irá enganar essas vítimas através, por exemplo, de identificações falsas, conseguindo a sua confiança, o seu carisma ou despertando sua curiosidade ou senso de urgência.

O primeiro ataque (que seria a isca propriamente dita) pode ser feito através de um telefone ou e-mail por exemplo. Mas, não se resumem a isso. Um outro exemplo de isca pode ser um simples DVD ou pen drive deixado pelo próprio fraudador na empresa. O fraudador pode, inclusive, conversar pessoalmente com algum funcionário e depois deixar com ele a isca. Expliquei isso em detalhes no capítulo anterior.

Mas, para dar embasamento à minha explicação, vou usar como exemplo os e-mails. O fraudador pode enviar milhares de e-mails por dia, para milhares de e-mails diferentes. Inclusive, no capítulo 02 tem

explicações de como os envios desses e-mails pode ser feito (e ressalto que não expliquei, obviamente, todas as formas possíveis). Só para citar como exemplo, uma das formas de se fazer isso é através de uma botnet. Mas, a forma com que os e-mails podem ser enviados não importa agora.

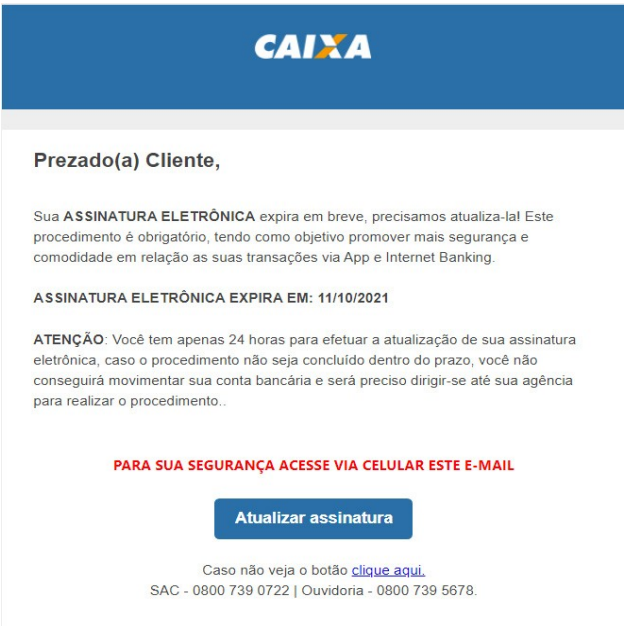
E um detalhe muito importante: o e-mail costuma imitar serviços e empresas conhecidas. Por exemplo: vamos supor que o conteúdo do e-mail seja de algum banco conhecido. O remetente deste e-mail pode imitar o e-mail do próprio banco, para fazer você pensar que foi o próprio banco que fez o envio. O endereço no campo remetente será um e-mail muito parecido com o do banco, utilizarão o logotipo e até a linguagem textual e visual serão parecidos.

O fraudador joga a isca. Essa isca sempre é bem trabalhada. No geral essas iscas usarão diversos gatilhos, como explorar a emoção, urgência e por aí vai. Não é qualquer isca. Você **não vai** receber um e-mail tipo, "oi, tudo bem? Clique aqui nesse link por favor?".

Ao invés disso, os e-mails serão carregados de senso de urgência, explorarão todas as suas emoções, provocará em você o terror, o medo, a dúvida, a ganância, te deixarão inquieto e ansioso. Você receberá e-mails tipo:

- Tribunal Regional da 2ª Região;
- Bloqueamos um acesso suspeito;
- Detectamos uma atividade incomum;
- Pagamento do pedido;
- Acesso suspeito em sua conta;
- Pedido em processo;
- Você foi selecionado para ser um cliente Bradesco (ou outro) Prime;
- Notificação do prêmio internacional de caridade eletrônica;

- Pix recebido;
- Intimação judicial;
- Intimação judicial do trabalho;
- Backup de histórico de conversas do Whatsapp;
- Pague seu cupom Uber;
- Assinatura suspensa;
- Assinatura NetFlix Suspensa;
- O procedimento é necessário para evitar o bloqueio de sua conta (o destinatário, de forma falsa, é de “algum banco”);
- Queixa crime em seu CPF/E-mail;
- Comprovante de transação bancária;
- Bloqueio Informe (afirmações de que sua conta no banco será bloqueada);



Exemplo de e-mail falso da Caixa.

- Cópia do cheque devolvido;
- Correios - Urgente! Notificação de mercadoria devolvida;
- Depósito nominal efetuado;
- Você recebeu um vale presente!
- Nosso segredo!
- Procedimento investigatório Nº "xxx";
- Achei sua foto, posso postar no face? rrssss;
- Entre centenas de outros exemplos.

Todos esses exemplos são reais. Desde 2008, cataloguei mais de 250 tentativas de ataques só no meu e-mail pessoal, fora as que não registrei.

Depois que a vítima receber o e-mail e abrir, três situações podem acontecer:

- **O e-mail conter algum anexo:** que será algum tipo de vírus;

- **O e-mail conter algum link:** que irá levar para uma página falsa onde poderá baixar algum vírus para o sistema ou pode ser algum página para enganar e capturar dados do cliente;

- **O e-mail conter algum anexo e link:** para ter os dois elementos, aumentando a chance de contaminação de roubo de informações.

Se for vírus, pode ser qualquer tipo de vírus. Neste caso você deve estudar, caso ainda não tenha feito isso, o capítulo 02.

Porém, estou falando agora sobre phishing. Portanto, o e-mail levará para uma página falsa. Essa página, pode, por exemplo, imitar uma página de algum banco. O e-mail recebido pode, por exemplo, pedir para que você clique no link e atualize dados cadastrais, caso

contrário a conta bancária pode ser desativada. Porém, se você digitar os dados na página falsa eles serão capturados.

Não é necessário dizer, mas farei assim mesmo, pois isso é óbvio, que as empresas que tem os nomes usados, como bancos, não tem envolvimento com esse e-mails e sites fraudulentos. Fica aí a dica.

O phishing conta ainda conta com três práticas ou técnicas mais elaboradas:

- **Pharming:** nesta técnica envolve a contaminação do computador da vítima por um vírus. A partir daí, quando o usuário digitar no navegador e URL de um site, ele é redirecionado para um site falso. A chance do usuário sem enganado é maior;

- **Spear Phishing:** é quando a mensagem, um e-mail por exemplo, contém o nome, sobrenome, telefone e outros dados da própria vítima. Isso pode fazer ela acreditar que o e-mail é de fonte legítima;

- **Vhishing:** nesta técnica o telefone é usado. Os criminosos podem criar mensagens automáticas e ligar para diversos números (ou se eles tiverem um alvo específico, ligarão para ele). Se a vítima atender, poderá inclusive ser direcionada para um “atendente” que conversará pessoalmente com ela. E

poderá a partir daí conseguir informações sigilosas com a própria vítima.

Boleto Falso

Esse é outro tipo de golpe extremamente comum no Brasil. Arrisco a dizer que esse golpe seja até mais comum que a própria prática de phishing. E explico por que: esse golpe já é antigo. Mesmo antes deles virarem pragas nos e-mails, golpistas enviavam e-mails falsos para a casa da vítima. Ou seja, eles confeccionam boletos em formato impresso e enviavam via correios.

Portanto, o boleto falso pode chegar até você via e-mail, WhatsApp e até via correios. Caso ele seja pago, o dinheiro vai para o fraudador.

O boleto terá todos o seus dados: nome completo, endereço, CPF por exemplo. Terá códigos de barras, logomarca da empresa e tudo mais.

Quando eu digo que o boleto vai ter logomarca da empresa, me refiro ao seguinte: os fraudadores criarão um boleto se passando por algum serviço que você usa (ou não) ou produto que você comprou (ou não).

Pode acontecer de você receber um boleto de algum serviço que você realmente utiliza. Por isso é preciso estar atento e desconfie das seguintes situações:

1 - O boleto vier com valor diferente (do valor normal que você já paga ou deveria pagar);

2- Se os três primeiros números do código de barras forem diferentes dos e-mails que você já recebe. Os três primeiros números identificam o seu banco, é bem simples;

3 - Se o boleto estiver sem a senha de proteção, caso você receba eles (os originais) no e-mail sempre com senha de proteção e abertura;

4 - Se você receber boleto via e-mail ou WhatsApp sem ter solicitado anteriormente.

5 - Boletos de serviços que você não utiliza ou produtos que nunca comprou.

Exemplo de boleto falso recebido via e-mail. Neste caso, o boleto era de um serviço que eu realmente utilizo, porém, o valor cobrado era diferente.

O golpe do boleto falso pode usar, inclusive, o phishing. Ou seja, os fraudadores criarão e-mails e sites imitando os e-mails e sites originais, com logomarca e tudo mais. Nem sempre essas imitações serão fiéis aos sites, e-mails e serviços originais. Fique atento se notar diferenças na aparência do e-mail recebido.

Outro fato importante, no caso de e-mails (ou WhatsApp) recebidos: o boleto falso pode ser uma isca para a entrada de vírus no sistema da vítima. Nem sempre vai existir um boleto para ser pago.

Catfish

Esse golpe é bem comum em sites ou aplicativos de namoro/relacionamento.

O golpista cria um perfil falso, onde ela posta diversas fotos (que pode ser fotos de terceiros) para demonstrar que é uma pessoa super interessante e que possui todas as qualidades que a vítima procura.

O golpista terá todas as qualidades que a vítima procura.

Quando uma vítima se sentir atraída e fazer contato (e pode acontecer do próprio golpista fazer o primeiro contato), o golpista vai continuar fazendo o jogo da conquista: vai demostrar ser a pessoa mais interessante o possível. Que possui muitas qualidades. Que tem sucesso financeiro, é empresário, faz muitas viagens e tudo mais.

Ao ocorrer o primeiro encontro, muita coisa pode acontecer:

- A vítima descobrir que a pessoa não é exatamente como aparentava ser;

- A vítima não perceber que tem algo errado até sofrer algum tipo de golpe, no mesmo dia, como por exemplo, ser roubada;

- Ocorrer agressões e até assassinatos;

- A vítima continuar gostando da situação e o golpista passa a investir ainda mais no golpe. Há casos onde o golpista passa a namorar com a vítima e até noivar. Porém, durante todo o tempo, situações de roubo e crime acontecerão. O golpista, nesses casos, costuma aplicar grandes golpes financeiros.

Esse golpe causa enormes prejuízos financeiros e emocionais nas vítimas (além dos riscos de agressão e até assassinatos).

É algo que todos devem ter muito cuidado. Cuidado com os famosos "namoro à distância". Tem muitos casos de vítimas todos os anos. Veja esse caso do jogador de vôlei italiano Roberto Cazzaniga, que durante 15 anos acreditou que namorava (à distância) a modelo brasileira Alessandra Ambrosio. Ele chegou a enviar 700 mil euros (R$ 4,3 milhões) para a golpista:

https://www.cnnbrasil.com.br/esporte/quem-e-o-jogador-que-passou-15-anos-acreditando-namorar-alessandra-ambrosio/#:~:text=Compartilhe%3A,pela%20brasileira%20h%C3%A1%2015%20anos.

Via SMS

SMS significa **S**hort **M**essage **S**ervice, que em bom português é Serviço de mensagens curtas. Nada mais é que as mensagens de textos que podemos enviar e receber através de celulares, smartphones e qualquer dispositivo capaz de usar a rede de telefonia móvel.

Os golpes via SMS no geral farão uso do phishing para tentar roubar informações do usuário. Geralmente são mensagens contendo links que levará para uma página falsa.

A partir daí você já conhece a história. Será solicitado para atualizar seus dados, solicitará informações sigilosos como dados do cartão.

As mensagens são diversas, há vários outros exemplos. Uma bem comum é a mensagem afirmando que a vítima possui pontos de fidelidade, e que eles precisam ser resgatados com urgência, pois estariam próximos do vencimento. Se a vítima clicar no link irá uma página falsa com o objetivo de capturar informações, tais como CPF, o número da agência bancária e conta corrente, além da senha de 8 ou 6 dígitos.

Golpe dos pontos de fidelidade.

Atualmente existem empresas especializadas em fornecer sistemas para envio de mensagens SMS em massa, ou seja, para centenas ou milhares de números de telefones. Essas empresas cuidam da estrutura de envios e não do conteúdo que os clientes enviam.

Além disso, programadores que já possuem um bom nível de entendimento de linguagens tais como o PHP conseguem criar seus próprios sistemas de envio de SMS em massa. Caso você queira entender um pouco mais sobre o que estou falando, pesquise no Google (www.google.com.br) por:

- Envio de SMS em via php;
- API para enviar SMS.

É possível contratar um serviço de envio de SMS ou até mesmo construir o próprio sistema através de linguagens tais como o PHP.

Golpe do Emprego

É fato que o emprego está alto no país. E muitos estão buscado a todo custo alguma forma de se recolocar no mercado de trabalho.

Muitos optam em trabalhar por conta própria, abrem micro negócios, trabalham em casa e por aí vai.

E muitos continuam dia após dia atrás de um emprego. Muitos golpistas percebendo isso usam o golpe do emprego: eles oferecem uma "vaga garantida", porém, para ter acesso a tal vaga é necessário pagar o acesso a algum sistema ou comprar um curso.

Atenção: **não** estou dizendo que comprar um curso para aprender a fazer algo, dominar uma técnica e se especializar, para aí sim ter uma maior chance de consegui um emprego, é errado. Estudar é excelente, aprender coisas novas é sempre bem vindo. Você pode até

despertar o seu lado empreendedor. Estude sempre, através de cursos presenciais, cursos online, livros impressos e livros digitais.

O golpe aqui mencionado é diferente disso. O golpe promete uma vaga de emprego "garantida". Por exemplo: oferece uma vaga "garantida" de recepcionista. Só que, para ter direito a vaga será necessário pagar alguma coisa e no final você descobrirá que nunca existiu uma vaga "garantida" para você. Geralmente eles cobram para ter acesso a algum sistema ou para fazer um curso. Só que esses valores são cobrados de centenas de pessoas. Quantas vagas "garantidas" eles tem??? O golpe está aí…

O golpe do emprego já é antigo e conhecido. Infelizmente os golpistas se aproveitam da fragilidade das pessoas, que estão desempregadas, buscando recolocação no mercado e muitas já não sabem o que fazer. Essas são as principais vítimas.

Golpe do WhatsApp

A mecânica básica desse golpe é a seguinte: o golpista investiga a vida de uma pessoa que terá o seu nome e fotos usadas para criar um perfil falso. E ele faz isso através das redes sociais, pois, a vida de muitos está toda lá: através das redes sociais é possível descobrir parentes, amigos, cidade onde mora, terá acesso a muitas fotos, etc.

Além de investigar a vida dessa pessoa, o fraudador investiga a vida de seus amigos e familiares (que serão aos mais lesados). Ele precisa descobrir nomes, cidades onde moram, número de telefone e tudo mais que for possível.

Com toda essa base de dados em mãos, ele (o golpista) cria um novo perfil no aplicativo, usando o nome e fotos da pessoa.

A partir daí ele passa a entrar em contato com os amigos e familiares dela dizendo que trocou de número de telefone. E que o número antigo deve ser apagado.

A partir daí o golpista começará a criar situações para pedir dinheiro para os parentes e amigos.

Esse golpe pode ter outras formas de funcionar. Há inclusive o roubo de contas, ou seja, quando o usuário tem seus dados de acesso copiado (por vírus por exemplo).

Por isso é importante sempre usar autenticação de dois fatores para aumentar a segurança.

Muitos amigos e familiares da pessoa que teve o nome e fotos usadas para criar um perfil falso acabam tendo algum prejuízo, seja através da transferência de valores em dinheiro ou pagamento de boletos.

Falsas mensagens de celular infectado

Essas mensagens podem aparecer sob a forma de um anúncio dentro de algum site que você esteja no momento. Portanto, se surgir mensagens como essas que cito aqui, não clique sobre elas. O seu celular/smartphone não está contaminado com nenhuma ameaça, a não ser que você clique no anuncio.

Podem surgir mensagens dizendo que seu aparelho possui algum vírus, problema no chip ou na bateria. Ou outros tipos de mensagens, fique atento.

Essas mensagens usam o gatilho da urgência, fazendo com que muitos cliquem nela. Ao clicar eles são direcionados a alguma página para instalação de algum app e/ou antivírus. Só que na verdade, esse tal app e/ou antivírus é o próprio vírus camuflado. Pode ser um malware ou spyware que irá espionar e copiar dados pessoais do usuário do aparelho.

Exemplos de mensagens.

Golpe do investimento em ação ou criptomoeda

Essa fraude/golpe já é muito conhecida, mas infelizmente continua causando transtornos e prejuízos para muitos. Você precisa ter muito cuidado se deseja entrar nesse mercado.

O golpe consiste em fazer uma falsa promessa de **retorno garantido ao investir em determinada ação ou criptomoeda**. Os golpistas farão todo um discurso de autoridade, demostram uma vida de riqueza e faz as possíveis vítimas sonharem com muita riqueza, prosperidade, vida boa, viagens, carros, e tudo mais.

Eles irão recomendar investimentos que em um primeiro momento pode até se demonstrar promissor, mas com o passar do tempo você perceberá que caiu em uma grande cilada.

O golpe está no fato de fazer **promessas de retorno garantido** e, principalmente, **as pessoas envolvidas não vivem de fato de investimentos**, **elas próprias não tem resultados com**

investimentos. **São vendedores de curso**. Elas ganham dinheiro é vendendo o curso, e não tem resultados reais.

O golpe está na promessa de retorno garantido...

Portanto, se pretende investir em ações ou criptomoedas, procure pessoas e/ou empresas sérias, que realmente são envolvidos com isso e que realmente tem resultados.

Por fim, vender cursos e treinamentos NÃO é errado. O golpe não está no curso/treinamento. Você pode comprar um curso sem a ilusão de ter resultado garantido e ficar milionário. Estudar não tem nada de errado. Você pode fazer cursos presenciais, online, assistir vídeo aulas, ler livros impressos ou digitais, etc. Profissionais/empresas que estão trabalhando de forma séria, comprometida, que são envolvidos com investimentos, NÃO estão fazendo nada de errado ao criar cursos e consultorias. Há muitas profissionais e empresas sérias no mercado, que trabalham com investimentos de fato, que estão comprometidos, que conseguem ter resultados reais e que não trabalham vendendo falsas promessas de riqueza e prosperidade em pouco tempo. Pesquise ao máximo e procure ter contato com essas

empresas e profissionais que fazem um trabalho limpo, transparente e pautado na verdade.

O golpe está na venda da falsa promessa, em todo o engano e ilusão criado nas vítimas e na geração do prejuízo financeiro que acabei de ressaltar.

Golpe do falso investimento

Aqui, neste tipo de golpe, os prejuízos são maiores. A promessa aqui é lucrar alto com investimentos. Por trás de tudo isso, falsas empresas (e pessoas) de consultoria financeira. Centenas de pessoas perderam tudo que investiram.

As vítimas depositam seu dinheiro em um falso investimento. Em alguns casos registrados e televisionados, as vítimas foram atraídas pela promessa de que, ao depositarem um certo montante, iriam "lucrar" todo mês um bom valor e depois de 12 meses receberiam o montante depositado inicialmente de volta.

Há um caso real e registrado (e você pode verificar a matéria no site: https://globoplay.globo.com/v/9644522/) de uma jovem que recebeu R$38.000,00 de herança do pai e não sabia como investir esse dinheiro. Infelizmente ela recebeu uma indicação de um amigo de infância para "investir" em uma suposta "empresa de consultoria financeira". A promessa da tal empresa:

- Ela investiria todo o montante de R$38.000,00;
- Iria receber (via depósito) R$1.040,00 todo mês e durante 1 ano;

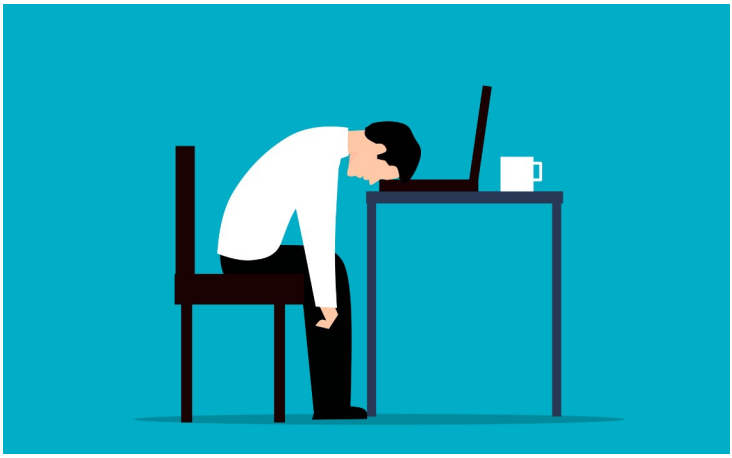
- Depois de 1 ano receberia os R$38.000,00 de volta;

- Nos primeiros meses o depósito foi feito na conta como o prometido. Alguns meses depois começou a ter atraso nos depósitos e por fim não houve mais nenhum depósito;

- A vítima resolveu ir até a sede da empresa e descobriu que já não existia mais nada. A empresa fechou as portas e os sócios/donos desapareceram sem deixar nenhuma explicação;

- Vários outros clientes foram lesados, inclusive funcionários da própria empresa que não tinham relação com o golpe.

Eu, Silvio Ferreira, NÃO entendo sobre investimentos. Mas, isso que essa "empresa de consultoria financeira" prometia representa algo em torno de 2.7% de rendimento por mês, ou 32.4% ao ano. Pense um pouco: isso parece algo seguro? E realmente não era seguro, pois foi um golpe, fraude e roubo de fato.



O golpe: as vítimas depositam seu dinheiro em um falso investimento.

Pense mais um pouco: um dos nomes mais respeitados do mundo dos investimentos, Warren Buffett (conheça história do maior investidor de todos os tempos: https://www.infomoney.com.br/perfil/warren-buffett/) consegue uma média de 20% ao ano nas últimas cinco décadas. E a tal "empresa de consultoria financeira" já promete 32.4% ao ano garantido?

Tudo que falei no tópico anterior vou repetir aqui: se pretende investir em ações ou criptomoedas, procure pessoas e/ou empresas sérias, que realmente são envolvidos com isso e que realmente tem resultados.

E aqui vale um adendo: não confie na primeira empresa ou pessoa que você tenha contato sem antes pesquisar muito. Não confie cegamente em "indicações" de amigos, pois, eles podem estar no mesmo engano que você. Pesquise, investigue, procure pelo histórico dos envolvidos. Procure conversar com pessoas já experientes na área. Se possível, participe de um bom curso ou treinamento antes para entender mais sobre o mercado de ações e investimentos. E óbvio, procure esses treinamentos com pessoas e empresas de confiança.

E mais um adendo: essas "empresa de consultoria financeira" falsas muitas vezes são, na verdade um, grande esquema de pirâmide financeira. Ler próximo tópico.

Esquemas de Pirâmide Financeiras e Marketing Multinível

A primeira questão que ressalto e deixo claro é que marketing multinível não é golpe. Incluir ele aqui porque sei que muitos não entendem a diferença entre um e outro.

O marketing multinível é um modelo de vendas totalmente legal, onde os integrantes/afiliados venderão algum produto e ganharão uma comissão. Além de ganhar comissão pela vendas dos produtos, o afiliado ganha comissões das vendas dos afiliados que ele conseguir trazer para o negócio.

Ou seja, além de eu ganhar dinheiro com as minhas vendas, ganharei um percentual sobre as vendas dos afiliados que eu conseguir trazer para o negócio.

Ou seja, a renda do marketing multinível está na venda de produtos. E quando há taxa de adesão é um percentual muito menor em relação à arrecadação com venda de produtos. A arrecadação no marketing multinível não está em taxas de adesão. Só para você ter ideia, nos EUA há uma regra que estabelece que pelo menos 70% da receita seja originada das vendas dos produtos e somente o restante é taxa de adesão. Se for algo fora desse padrão já é considerado pirâmide financeira.

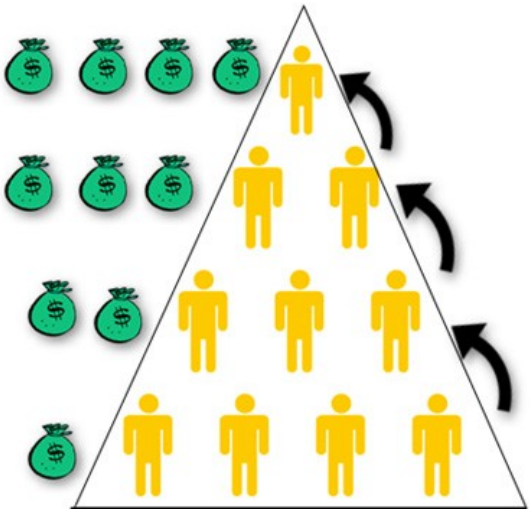
Basicamente é isso. É bem tranquilo de entender e diferenciar em relação a esquemas de pirâmides financeiras.

As pirâmides financeiras por sua vez, são crimes. São proibidas. E todos os anos têm pessoas levando prejuízo, pessoas fugindo do país e pessoas sendo presas.

A pirâmide financeira lucra com a adesão de novos membros. A lucratividade não está em venda de produtos, mesmo que exista um produto sendo ofertado. Basicamente, uma pirâmide financeira é:

Um tipo de esquema que tira proveito em recrutar pessoas com a promessa de ganho fácil. O dinheiro vem da adesão de novos membros. Quem está no topo, ganha a comissão de todos os que

estão abaixo dele. Quem está no topo sempre ganha mais. E conforme você vai entender algumas linhas à frente, vai chegar um ponto onde não tem mais como expandir a pirâmide, causando assim o total colapso do esquema, prejuízo e frustração de quem está na parte de baixo.



Nesse tipo de golpe, quem está no topo sempre ganha mais.

Fiz um resumo de como funciona esse esquema:

1 - Geralmente você vai receber o convite através de algum "amigo", parente ou outra pessoa que já faz parte do esquema. Ele pode até afirmar que se trata da venda de algum produto (mas o que movimenta o negócio são as taxas de adesão). Mas ele é apenas um chamariz. Não é a sua venda que "sustenta" (entre aspas. Esses esquemas são impossíveis de se sustentar) a pirâmide;

Outra forma de receber o convite é através de e-mails e anúncios que podem camuflar o esquema (falo sobre a questão da camuflagem um pouco mais adiante). Antigamente era comum usarem cartas que eram enviadas através dos correios.

2 - Você ouvirá a promessa de lucros mensais muito atrativos, retenção de capital investido e promessa de ganho extra através da indicação de novos clientes;

3 - Se você entrar no esquema, fará o pagamento da taxa de adesão. Essa taxa de adesão pode estar disfarçada de "compra de algum produto" ou algum tipo "investimento";

4 - A partir daí muitas coisas podem acontecer. Você pode querer participar ativamente do esquema e começar a indicar outros amigos e conhecidos. Dessa forma você também ganharia por cada pessoa que entrar. E quanto ao produto ofertado? A essa altura você não quer nem saber de produto. O mais importante agora seria trazer novos membros;

5 - É da taxa de adesão dos novos associados que virá o dinheiro que remunera quem já é membro. No tópico anterior abordei sobre o golpe do falso investimento. Neste caso o pagamento do associado deveria ser todo mês, durante um ano. Esse dinheiro vem justamente da taxa de adesão que foi cobrada, que é o valor inicial que a vítima depositou de boa fé;

6 - Na medida que novos membros entrarem no esquema, cresce a base dos associados. E portanto, mais pessoas que deveriam receber algum valor todo mês;

7 - Quanto mais o esquema crescer, mais ele se torna insustentável. Isso ocorre por um motivo bem simples: a capacidade de atrair novos membros constantemente de cada pessoa atinge o limite. E o pagamento dos associados começa a atrasar. Se não há novos membros em quantia suficiente, não tem como pagar quem já faz parte do esquema. Os primeiros a levar prejuízos são os de parte debaixo da pirâmide;

8 - Com o atraso nos pagamentos, a desconfiança aumenta e o número de novos associados diminui drasticamente;

9 - Por fim, a pirâmide se torna insustentável, os pagamentos são cessados e os principais sócios (os donos do esquema, que estão no topo da pirâmide) desaparecem. Obviamente os sócios principais (os que estão no topo da pirâmide) são os únicos a lucrar nesse momento. Dependendo do tamanho da pirâmide, o golpe é de milhões;

9 - Os associados lesados descobrem que caíram em um golpe;

10 - Neste ponto, as vítimas começam a tentar fazer contato com os responsáveis e descobrem que a sede da empresa e/ou escritório foram fechados às pressas e os sócios/donos desapareceram.

Tenha extremo cuidado para não cair nessa cilada. Toda pirâmide vai chegar em algum dado momento que se tornará insustentável e irá ruir, desabar. E aí, todas as pessoas que você tiver trazido para a pirâmide culparão você. Você está acima delas, é o contato que elas tem. Isso é crime, dá processo e cadeia.

Anteriormente mencionei que esses esquemas de pirâmides podem chegar até você de forma "camuflada". E é o que acontece. Ninguém vai te abordar e dizer "topa entrar em um esquema de pirâmide financeira comigo?"

Ao invés disso, o esquema será disfarçado de outros tipos de negócios que são legais e permitidos. O negócio será apresentado de forma muito bem elaborada, com uso de argumentos totalmente lícitos e coerentes. Você, em um primeiro momento, não perceberá que está participando de algo que é crime. Muito pelo contrário: irá se sentir até empolgado com a ideia, com a nova possibilidade de ganhar dinheiro, afinal, é algo novo para você, é uma nova forma de trabalhar.

Mas, quais são os principais tipos de negócios lícitos que as pirâmides financeiras podem se disfarçar? São eles:

1 - Aplicações financeiras: muito comum e no tópico já mencionei sobre isso. São as famosas falsas "empresa de consultoria financeira". Você faz o investimento de um valor inicial, ganharia um excelente rendimento mensal e depois de um acerto tempo teria o valor inicial devolvido. É um golpe antigo, bem manjado, mas que infelizmente faz muitas vítimas todos os anos;

2 - Marketing multinível: já expliquei o que é marketing multinível. Ele é um negócio legal, não é crime. Mas, como forma de enganar os envolvidos, muitos esquemas de pirâmide financeira se disfarçam, se camuflam e se travestem de marketing multinível. Isso se torna evidente quanto a empresa responsável cobra valores para a adesão de novos associados, que nesse ponto costuma ser chamado de afiliados. E a arredação financeira dessa empresa consiste em sempre conseguir novos afiliados. Ou seja, ela fatura mais com a adesão de

novos afiliados do que com a venda de produtos. Quando isso acontece é definido como pirâmide financeira.

Golpes do FGTS

Mais um golpe que não é nenhuma novidade, mas que infelizmente segue fazendo muitas vítimas. O pagamento do saque do FGTS é feito de forma automática em conta poupança digital no aplicativo Caixa Tem. O golpe ocorre quando terceiros (golpistas) conseguem transferir o dinheiro pelo aplicativo de pessoas que ainda não fizerem a retirada dos valores que eles tem direito.

Esse golpe possui várias fases. Não é algo simples, e quando chega na fase final (quando o golpista transfere o dinheiro do caixa Tem) é porque a vítima já caiu em outras armadilhas e iscas. Por isso a importância de estudar um livro como este que se encontra com você, entender os vários riscos e passar a ter mais atitudes de segurança.

Agora, veja passo a passo como o golpe funciona:

1 - O golpista precisa ter acesso ao os dados das vítimas para ter acesso ao app Caixa tem;

2 - Para ter esses dados, ele vai utilizar diversas técnicas de roubo de informações diretamente do celular, tablet ou computador das vítimas, tais como:

2.1 - Engenharia social;
2.2 - Phishing;
2.3 - Vírus.

3 - Com os dados da vítima em mãos, ele acessar o app Caixa Tem e transfere o dinheiro para outra conta.

O golpista precisa ter os dados da vítima. Com posse dessas informações ele consegue acessar o Caixa Tem e transfere o dinheiro para outra conta.

Isso que acabei de explicar é a mecânica do golpe. Na prática, ocorre o seguinte: o criminoso envia para as vítimas e-mails se passando por alguma empresa conhecida, como a própria Caixa Econômica Federal.

Neste e-mail há uma mensagem solicitando cadastro, alguma mensagem que chame a atenção, uma proposta/oferta de saques de valores maiores, oferta de antecipação do saque do FGTS, etc.

E haverá um link para fazer algum tipo de cadastro. Se a vítima clicar e preencher os dados, o criminoso estará de posse de todos os dados necessários para acessar o app Caixa Tem.

Muitas pessoas foram vítimas desse golpe por acreditar que os e-mails recebidos eram verídicos. Principalmente porque há instituições sérias, que fazem um trabalho sério e profissional e que oferecem a opção de antecipar a retirada do valor. Quer um exemplo: PicPay. O importante é saber diferenciar esses e-mails maliciosos dos e-mails verdadeiros. Na dúvida, acesse o site oficial da empresa envolvida, digitando a URL em seu navegador e entre em contato com o suporte no telefone ou no chat. Procure os canais oficiais de atendimento, cheque se as propostas e e-mails recebidos são verdadeiros. É bem simples.

Aumento de Limite de cartão e Falso Empréstimo

Esses golpes se resumem a phishing e, consequentemente, roubo de informações.

Já abordei, anteriormente, sobre o phishing, e tudo que expliquei vale para esse tópico. Esse tópico serve para chamar a sua atenção, devido a seriedade do golpe.

Golpistas usarão de phishing para criar e-mails e websites se passando por instituições financeiras e operadoras de cartões de crédito. A oferta: empréstimos com juros baixos, aumento de limite de crédito em cartões, etc.

E como você já deve imaginar, eles solicitam algum cadastro. E neste ponto ocorre o roubo de informações que seriam digitadas pela própria vítima.

Por isso, cuidado ao receber e-mails dizendo que você possui algum tipo de crédito pré-aprovado, aumento de limites e por aí vai.

Isca recebida em meu e-mail. Detalhe: não tenho conta nesse banco e meu e-mail não é cadastrado nele.

Outros Golpes Whatsapp

Neste ponto do livro você já consegue entender, e muito, o funcionamento de golpes envolvendo computadores, tablets, celulares, phishing, vírus e muito mais.

Esse tópico, assim como o anterior, serve para chamar a sua atenção, devido a seriedade de golpes envolvendo o Whatsapp.

No geral, desconfie de qualquer link que receber, fique atento. Desconfie de mensagens, pedindo para você fazer alguma coisa, baixar algum app, fazer alguma atualização, enviar algum código e etc.

Só para você ter ideia, existe um outro golpe onde entrarão em contato com você solicitando, via Whatsapp ou SMS, podendo inclusive usar phishing e muita técnica de persuasão. Você pode ser convencido clicar em algum link, instalar algum app e enviar um código de verificação no final.

Se fizer isso, o fraudador conseguirá se conectar no Whatsapp e ter acesso a todo os contatos do seu Whatsapp, conversas, número de telefones, etc. Ou seja, você terá o seu perfil sequestrado.

Golpes no Instagram

Tudo que mencionei no tópico anterior aplica-se a este tópico. Inclusive há alguns golpes que se utilizam exatamente da mesma técnica. Vejamos alguns:

Sequestro de perfil

Neste caso o fraudador conseguirá se conectar na sua conta e você perderá acesso à ela. O fraudador passa a usar o seu perfil para fazer anúncios, pedir pix para amigos, e tudo mais.

Sempre usando a sua imagem. Todas as pessoas que te conhecem irão achar que é você oferecendo produtos para venda, pedindo pix, etc.

Veja um resumo de como funciona o golpe:

1 - O golpista criará um perfil fake (falso) de alguma **empresa** que você segue. Ele pode criar um perfil fake de **pessoa física** também. Ou seja, o golpista já segue você, já está investigando você;

2 - Ele vai usar, nesse perfil fake, a mesma imagem de perfil, vai subir as mesmas publicações e seguir as mesmas pessoas, igual ao perfil verdadeiro;

3 - Ele pode inclusive usar esse perfil fake para seguir você. Isso é feito na tentativa de fazer você seguir o perfil fake criado por ele;

4 - Agora que o palco está armado, o golpista segue para o próximo nível: ele entra em contato com você, usando o perfil falso. O teor desses contatos podem ser diversos. Mas ele pode, por exemplo, te avisar que irá ter alguma promoção na empresa, algum sorteio, algo que você com certeza irá querer participar. E ele pede o seu número de telefone;

5 - Se você enviar o número, o golpista já sabe que você caiu no golpe. A isca foi fisgada. O próximo passo: o golpista avisa que você vai receber um SMS com um link. E que você precisa copiar esse link e enviar para ele;

6 - Pode ter variações na abordagem. E neste meio tempo ele usará todas as táticas de persuasão que forem possíveis;

7 - Se enviar o link, você perde acesso ao seu perfil. O que o golpista fez foi redefinir os seus dados de acesso. O link recebido era para redefinição de senha de acesso, o recurso “Esqueci senha”.

O perfil fake criado pode ser de qualquer empresa. Pode ser inclusive do próprio Instagram. Há um caso real de uma pessoa que achou estar conversando com o suporte do próprio Instagram. Eles estavam oferecendo a conta verificada, aquele símbolo azul. E a vítima caiu exatamente no mesmo golpe e perdeu o acesso ao seu perfil.

Golpe do perfil verificado

Como você acabou de ler, o golpe anterior pode ter como isca a possibilidade do usuário ter conta verificada, aquele símbolo azul. Mas, usando essa mesma isca um outro tipo de golpe se tornou bem conhecido.

Redes sociais no geral possuem a possibilidade de ter o perfil verificado. É uma forma de atestar que a conta/perfil é original e pertence efetivamente a uma pessoa ou negócio.

Muitos querem esse selo, mas não é todos que conseguem. No caso do Instagram, não existe garantia que uma dada conta conseguirá esse selo.

Aí que entra o golpe: os golpistas podem se apresentar como "consultores de imagem" ou "figura pública" (só para exemplificar) e oferecer algum tipo de serviço que **"garantiria"** a aquisição deste selo e teria a conta verificada.

Saiba que o Instagram não cobra para atribuir esse selo nas contas, tampouco há garantias. É necessário ter uma análise pelo Instagram,

que solicitará alguns dados pessoais e um documento com foto, como RG, passaporte ou carteira de habilitação.

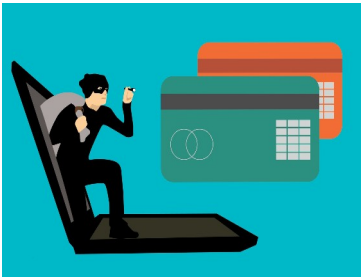
O próprio dono do perfil é quem deve solicitar essa verificação:

1: Acesse seu perfil do Instagram e clique nos três tracinhos, localizados à direita do seu nome;

2: Clique em Configurações;

3: Selecione Conta - Solicitar verificação;

Golpe do perfil hackeado



Neste tipo de golpe, o fraudador criará um perfil fake de alguma pessoa. Irá repostar todas as fotos e vídeos. Seguir as pessoas do perfil verdadeiro. Os "preparativos" iniciais são exatamente iguais do explicado em Golpe do perfil hackeado.

O que difere aqui é que o golpista não sequestrará a conta original. Ao invés disso ele tentará contato com as pessoas, pode ser desconhecidos, amigos e até familiares da vítima, dizendo que a sua conta/perfil foi invadida por hackers e ele teve que criar a nova conta urgentemente.

O golpista pode, inclusive, pedir para que as pessoas bloqueiem a "conta antiga" (que na verdade é a conta original).

A partir daí a história é a mesma. O golpista/fraudador poderá solicitar dinheiro emprestado e/ou pix dos amigos e parentes da vítima, iniciar outros ataques, etc.

Falso Motoboy

Esse é um golpe antigo e bem manjado. Mesmo assim continua a fazer vítimas.

O golpe funciona assim:

1 - Alguém vai te ligar fingindo ser de algum banco ou operadora de cartão de crédito dizendo que seu cartão foi clonado ou qualquer coisa parecida;

2 - Gatilhos de urgência, entre outros, podem ser usados para atrapalhar a sua tomada de decisão. Pode ser relatado que uma compra em um valor altíssimo já foi feita em seu cartão;

3 - Para resolver o problema, o golpista vai dizer que um motoboy irá até a sua casa para recolher o cartão para que o mesmo seja cancelado/bloqueado e substituído;

4 - Mesmo que você não forneça a senha do cartão, quebre-o ou corte-o ao meio, o golpista ainda poderá utilizá-lo para fazer compras na internet. Os dados necessários para realizar compras são: o número completo do cartão, o nome impresso, data de vencimento e código de segurança.

Outros Golpes, Fraudes e Falcatruas

Existem uma quantidade enorme de golpes, fraudes e falcatruas. Eu poderia escrever tranquilamente páginas e mais páginas de exemplo.

Porém, o livro pode ficar um pouco repetitivo e cansativo. Muitos golpes possuem "modos operantes" semelhantes. Veja:

- Uma quantidade enorme de golpes são no fundo phishing.
- Muitos possuem como objetivo roubar informações da vítima;
- Muitos podem utilizar algum vírus;
- Entre outras situações.

E tudo isso já foi estudado passo a passo. Ao estudar tudo que já foi exposto até ate aqui você já tem total capacidade de identificar qualquer tentativa de golpe. Ou pelo menos boa parte delas. Você já entende como eles funciona, os artifícios usados, os gatilhos, os vírus e tudo mais.

A partir deste ponto tenha bom senso e saiba identificar situações de risco de situações normais e que não representam um risco.

Muitas situações beiram o absurdo, mas muita gente é pega. Por exemplo: se você receber o seguinte e-mail:

- **O campo assunto preenchido:** "Nosso Segredo!"

- **E no corpo da mensagem vem escrito:** "Não sei porque você me pede essas coisas, está tudo aí do jeitinho que você me pediu. E por favor não mostra pra ninguém."

Você abriria o anexo ou clicaria no link? E se:

- Alguém disser que vai te dar muito dinheiro;
- Ou que ganhou na mega sena e precisa da sua ajuda para receber o prêmio.

Sempre analise cada situação, não tome decisões no calor da emoção. Tudo que é bom demais para ser verdade deve ser checado nas fontes originais.

Ser cuidadoso sim, cismado a ponto de achar que tudo na vida é golpe não. É preciso ter inteligência para ficar longe de golpes e não perder as boas oportunidades.

Oportunidades boas existem sim. Existem pacotes de viagem relativamente baratos? Sim. Existem empresas e pessoas que vendem cursos e treinamentos acessíveis e carregados de overdelivery? Sim. Existem boas oportunidades reais? Sim.

Leia e estude este livro o máximo que puder. Todo o conhecimento aqui disposto vai ajudá-lo a se manter sempre seguro.