CENTRO DE TREINAMENTO
MARCOS MONTEIRO

FORENSE

GOLPES NA INTERNET

CLONAGEM DE WHATSAPP

1. Para o WhatsApp identificar se o seu número de telefone de fato pertence a você, a ativação do aplicativo com seu número depende da confirmação de seis dígitos enviados via SMS, quem tiver acesso a esses seis dígitos será capaz de usar o aplicativo com seu número;

2. No começo, os golpistas com auxílio de algum funcionário da empresa de telefonia, agiam resgatando o seu chip (SIM CARD) para assim receber o 'SMS' contendo os dígitos de verificação do WhatsApp, porém, as empresas criaram mecanismos para dificultar esse procedimento. Os golpistas então passaram a se utilizar da técnica conhecida como "Engenharia ou Engenhosidade Social", um golpe que consiste em adquirir a sua confiança, para a partir dela, perguntar para você quais dígitos (os dígitos de verificação de WhatsApp) acabara de receber por mensagem de texto. Já pensou em ganhar do nada uma pizza, mas para tanto, necessita apenas confirmar a sequência de números que fora enviado diretamente para o seu celular? Se liga, tal ação se trata de um golpe!

Como evitar:

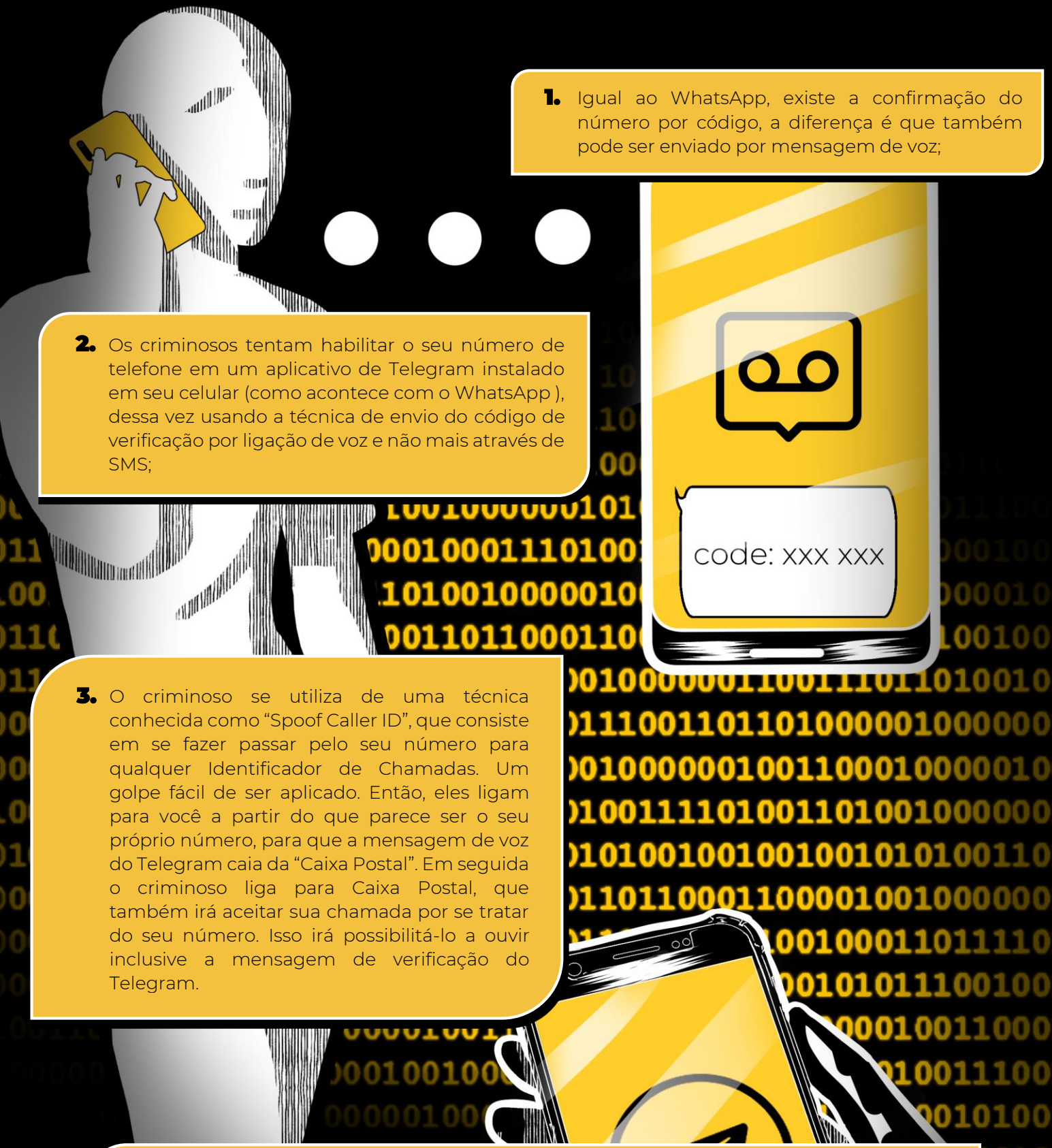
a) Em **Configuração de Conta** do seu WhatsApp, ative a opção "**Confirmação em duas etapas**", o aplicativo pedirá que cadastre uma senha de 6(seis) dígitos, além de um e-mail. **Evite senha com datas comemorativas ou números sequenciais**, isso dificultará o criminoso de ir adiante na clonagem do seu WhatsApp;

b) **NUNCA** informe os dados recebidos por SMS ou os cadastre em aplicativos de terceiros;

c) **Desative** as visualizações de mensagens e SMS na Notificação de tela de bloqueio;

d) Ao receber mensagens de ofertas, promoções, sorteios... Através de redes sociais ou por e-mail se identificando como funcionário de uma empresa, confirme o fato retornando a ligação para a própria empresa.

CLONAGEM DE TELEGRAM



1. Igual ao WhatsApp, existe a confirmação do número por código, a diferença é que também pode ser enviado por mensagem de voz;

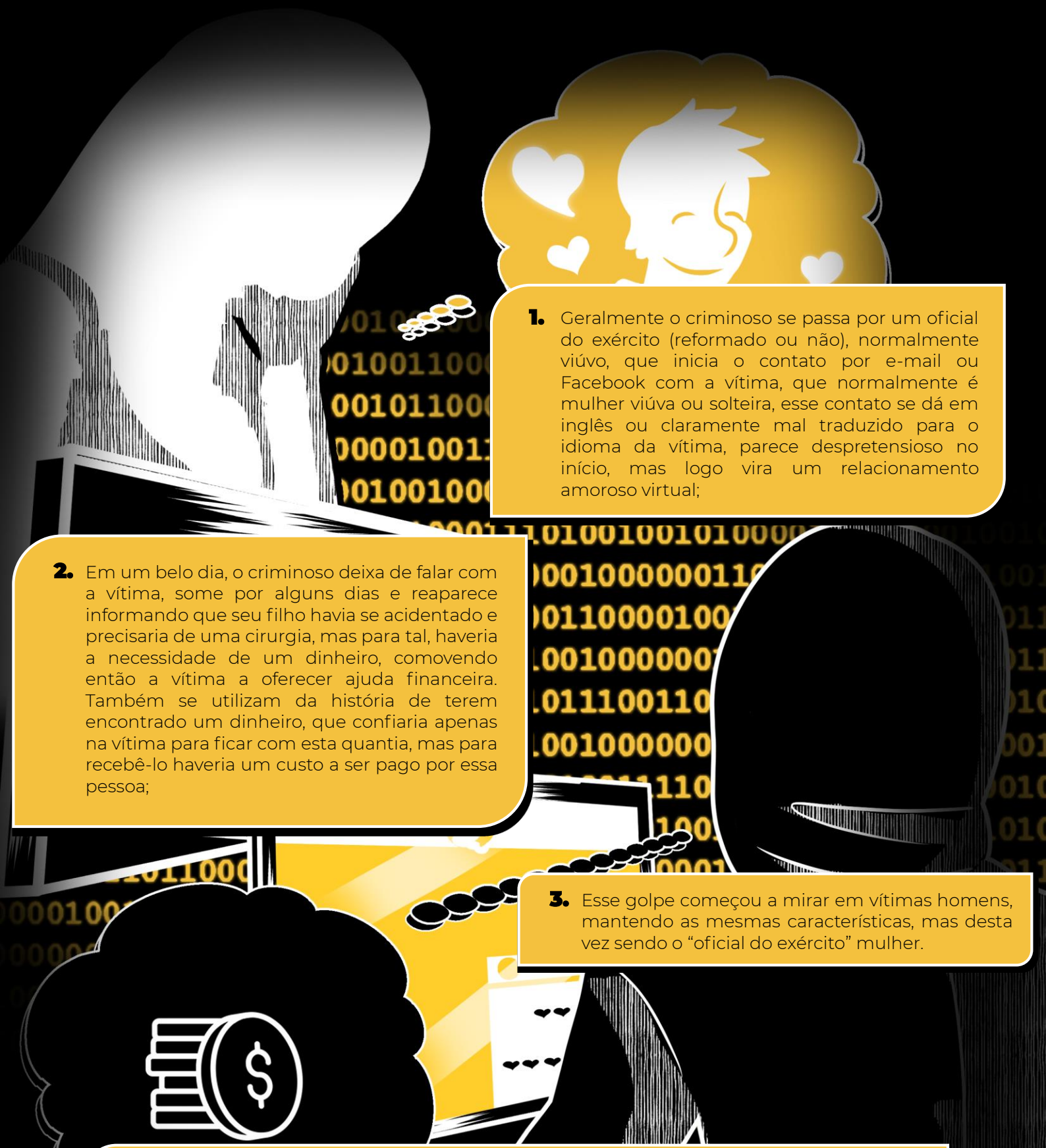
2. Os criminosos tentam habilitar o seu número de telefone em um aplicativo de Telegram instalado em seu celular (como acontece com o WhatsApp), dessa vez usando a técnica de envio do código de verificação por ligação de voz e não mais através de SMS;

3. O criminoso se utiliza de uma técnica conhecida como "Spoof Caller ID", que consiste em se fazer passar pelo seu número para qualquer Identificador de Chamadas. Um golpe fácil de ser aplicado. Então, eles ligam para você a partir do que parece ser o seu próprio número, para que a mensagem de voz do Telegram caia da "Caixa Postal". Em seguida o criminoso liga para Caixa Postal, que também irá aceitar sua chamada por se tratar do seu número. Isso irá possibilitá-lo a ouvir inclusive a mensagem de verificação do Telegram.

Como evitar:

a) Tal como acontece com o WhatsApp, na configuração de **"Privacidade e Segurança"** você pode habilitar a "**Verificação em Duas Etapas**";
b) Caso não use, solicite a sua operadora de Celular que sua **Caixa Postal seja desativada**;
c) **Jamais** atenda uma ligação do seu próprio número, caso venha a receber, agora você já sabe que é uma tentativa de golpe;
d) Você também consegue ver quais dispositivos estão conectados a sua conta simultaneamente na opção **"Dispositivos"** na configuração do seu Telegram.

GOLPE DO AMOR (SCAMMERS)



1. Geralmente o criminoso se passa por um oficial do exército (reformado ou não), normalmente viúvo, que inicia o contato por e-mail ou Facebook com a vítima, que normalmente é mulher viúva ou solteira, esse contato se dá em inglês ou claramente mal traduzido para o idioma da vítima, parece despretensioso no início, mas logo vira um relacionamento amoroso virtual;

2. Em um belo dia, o criminoso deixa de falar com a vítima, some por alguns dias e reaparece informando que seu filho havia se acidentado e precisaria de uma cirurgia, mas para tal, haveria a necessidade de um dinheiro, comovendo então a vítima a oferecer ajuda financeira. Também se utilizam da história de terem encontrado um dinheiro, que confiaria apenas na vítima para ficar com esta quantia, mas para recebê-lo haveria um custo a ser pago por essa pessoa;

3. Esse golpe começou a mirar em vítimas homens, mantendo as mesmas características, mas desta vez sendo o "oficial do exército" mulher.

Como evitar:

a) No Google imagens é possível fazer o upload da imagem e identificar se a foto de perfil se trata mesmo da sua identificação;

b) As mensagens enviadas normalmente são roteirizadas pela quadrilha, se copiar e colar o texto enviado pelo possível golpista no buscador de Internet Google é possível que já identifique se tratar de mensagem dos scammers.

SEXTORSÃO

1. Ocorre cada vez mais em plataformas como Tinder, Facebook ou Instagram, quando se conhece um(a) possível parceiro(a) que evolui para um relacionamento amoroso à distância, culminando em trocas de imagens ou vídeos íntimos, até que, de posse dos mesmos, o criminoso exige uma quantia para não divulgar as fotografias e vídeos da sua vítima;

2. Quando a vítima é homem, o caso é mais incidente pelo Facebook, inicialmente o criminoso se faz passar por uma bela mulher que o adiciona como amigo, logo puxa assunto e chama-o para uma conversa mais íntima por chamada de vídeo, na chamada de vídeo o que a vítima ver (sem saber) é uma gravação de uma mulher se despindo, incentivando a vítima a fazer o mesmo enquanto o criminoso grava as ações. Com a gravação (material necessário para o golpe) concluída, o criminoso encerra a ligação e exibe o conteúdo gravado, daí se inicia a extorsão.

Como evitar:

a) **Evite** compartilhar fotos e vídeos íntimos com desconhecidos;
b) Busque **investigar** se a pessoa do outro lado de fato é quem se diz ser. Fazer buscas por imagens no Google Imagem podem ajudar.

Ggolpe do Mercado Livre

1. O criminoso discretamente nos comentários do anúncio convence a vítima a fornecer o seu e-mail, normalmente atraída com a possibilidade de realizar a venda sem pagar ao Mercado Livre um percentual sob a operação;

2. A vítima então recebe um e-mail que parece ser do Mercado Livre, com o domínio do endereço de e-mail muito parecido, até mesmo igual as vezes, em seu conteúdo, o layout e as cores parecidas informando que a venda foi realizada, já fornecendo no e-mail o endereço para envio do produto;

3. Depois de algum tempo, após a vítima perceber que não houve o repasse do dinheiro pela plataforma, pois a venda nunca foi realizada, é que começa a entender ter sido vítima de um golpe.

Como evitar:

a) **Nunca** forneça a um possível comprador o seu e-mail ou até mesmo telefone em uma operação de venda do Mercado Livre;

b) Use apenas o aplicativo do Mercado Livre e Mercado Pago do Celular para **assegurar** se de fato a venda foi realizada;

c) Caso receba o e-mail, **procure um perito** para analisar seu cabeçalho para averiguar a origem real do e-mail.

E-MAIL FALSO

1. Um criminoso com conhecimento mais avançado pode produzir um e-mail cujo o seu endereço seja exatamente o endereço real, isso aumenta e muito o poder de convencimento, pois a vítima facilmente acreditará se tratar do endereço de domínio de um determinado banco ou e-commerce;

2. A vítima então recebe esse e-mail e nele pode conter anexado um software malicioso, um boleto falso ou um endereço de Internet levando-o a um site falso de banco ou de venda de produtos que nunca serão entregues.

Como evitar:

a) Verifique se seu provedor de e-mail faz consulta de DNS Reverso, apenas utilize provedores de e-mails que tenham isso habilitados;

b) Verifique se seu provedor de e-mail tem anti-spam e deixe-o habilitado;

c) Veja como pode analisar o "Cabeçalho do e-mail", este não se trata do remetente, se trata de exibir todo código do e-mail, cada cliente tem uma forma diferente para exibi-lo. Feito isso, copie e vá no site www.marcosmonteiro.com.br, no menu FERRAMENTAS > FORENSE NA INTERNET > CABEÇALHO DE E-MAIL, em seguida cole todo o cabeçalho, a ferramenta te ajudará a entender a origem do e-mail.

BOLETO FALSO

1. O criminoso cria um e-mail falso da empresa de telecomunicações, com um boleto falso do valor a ser pago apontando para outra conta bancária;

2. OU o criminoso envia um e-mail se fazendo passar por uma empresa de cobrança, no qual oferece um acordo, em anexo um boleto falso;

3. OU o e-mail de cobrança é verdadeiro - sem boleto em anexo, mas com um link de geração automática do mesmo, porém um Malware na máquina da vítima pode alterar o código de barras no ato da geração;

4. OU o e-mail de cobrança é verdadeiro e o boleto foi gerado pela empresa de cobrança, enviado em anexo, porém o boleto foi adulterado por um malware na origem.

Como evitar:

a) Observe no ato do pagamento se o banco identificado na leitura do código de barras é o mesmo que aparece na impressão do boleto;
b) Quando possível, identifique se o cedente, que também pode ser chamado de beneficiário do boleto é mesmo o provedor do serviço ou produto contratado;
c) Observe se o número impresso no boleto é o mesmo que o lido pelo código de barras;
d) Sempre guarde o boleto recebido para uma possível cobrança futura.

GOLPE DA OLX (COMPRA DE VEÍCULOS)

1. Geralmente feita na OLX, o criminoso age em duas frentes, para o vendedor original ele se apresenta como comprador. De posse de todas as informações do veículo ele cria um anuncio com o mesmo produto e preço mais atraente para então buscar uma outra vítima – um possível comprador de fato;

2. Quando aparece o comprador interessado no veículo, o criminoso então começa a intermediar para que as duas vítimas se encontrem apenas para apresentar o produto. A compra uma vez efetivada, a vítima não recebe o produto, pois o pagamento foi para o criminoso que "intermediou" a compra e não para o vendedor de fato, que nesse caso também foi vítima.

Como evitar:

a) Nunca divulgue a placa do veículo (ela pode ser usada em outros golpes, como a de clonagem de placas);

b) Analise o documento do veículo, consulte no site do departamento de trânsito a veracidade do mesmo, confrontando PLACA, CHASSI e proprietário do veículo com seu documento de identificação (para garantir que esteja mesmo tratando com a pessoa certa);

c) Consulte se há outros anúncios do mesmo veículo, é possível consultar até mesmo pela imagem apresentada do mesmo no Google Fotos;

CENTRO DE TREINAMENTO
MARCOS MONTEIRO

CONTATO

WWW.**MMFORENSE**.COM

Geral:
+55 (11) 3164-7815 | +55 (11) 9 8940-2000
Pericias:
+55 (11) 9 8940-2000
Cursos:
+55 (85) 9 9439-0601 | (85) 9 9415-9544
Marcos Monteiro:
+55 (85) 9 8805-4112

Cursos:
comercial@marcosmonteiro.com.br

Marcos Monteiro:
contato@marcosmonteiro.com.br

FORENSE

@**mmforense**

in/**marcosjmonteiro**

facebook.com/**mmforense**

youtube.com/**marcosmonteiro**

Sede em São Paulo:
Av. Paulista, 1842 , Conj. 155,
15° andar, Torre Norte;
Bela Vista - CEP 01310-945
São Paulo SP;

Sede em Fortaleza:
Rua Petrônio Portela, 200,
Edson Queiroz;
CEP 60834-425
Fortaleza - CE;