SEGURANÇA CORPORATIVA
A TECNOLOGIA A SERVIÇO DO CRIME

Nos tempos atuais vivemos tentando nos proteger de um inimigo quase invisível.

Estamos falando dos crimes onde são utilizados meios tecnológicos para o seu cometimento, onde muitas das vítimas, ao perceberem que estão sendo vítimas, não conseguem cessar o prejuízo.

Nas corporações não é diferente, quanto mais preparados são estes criminosos mais alcançam grandes empresas e causam enormes prejuízos.

A proteção está nos treinamentos contínuos e na prevenção com suporte da tecnologia.


CRIMES COM USO DA TECNOLOGIA
Clonagem do WhatsApp
Boleto Falso
Fraudes Bancárias
Sextorsão
Golpe do Falso Leilão ou Falso Empréstimo

CRIMES COM USO DA TECNOLOGIA

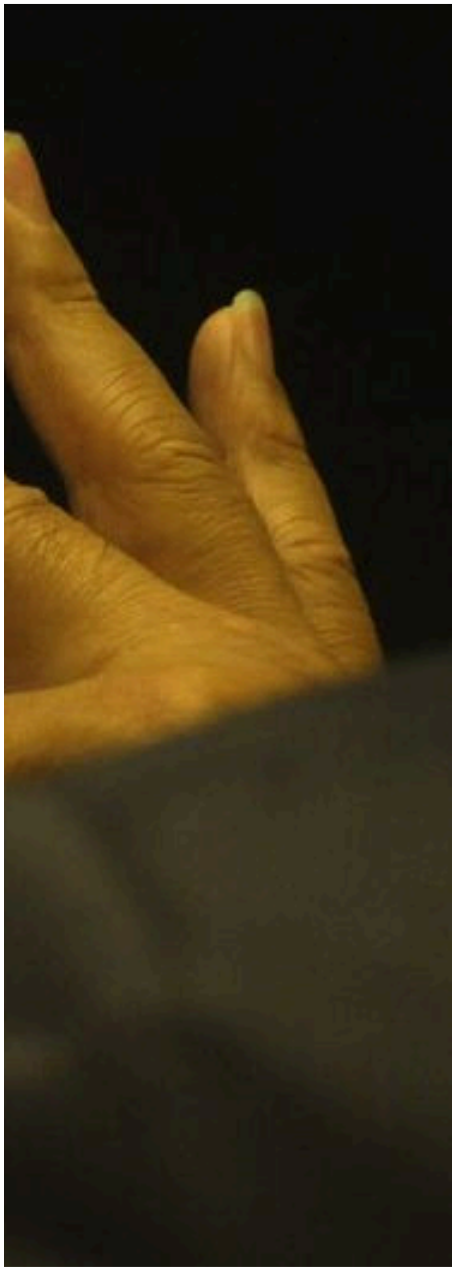
- Golpe do Amor – Golpe Don Juan
- Ransomware
- Sites de Comércio Eletrônico Fraudulentos
- Golpes envolvendo PIX

CLONAGEM DE WHATSAPP

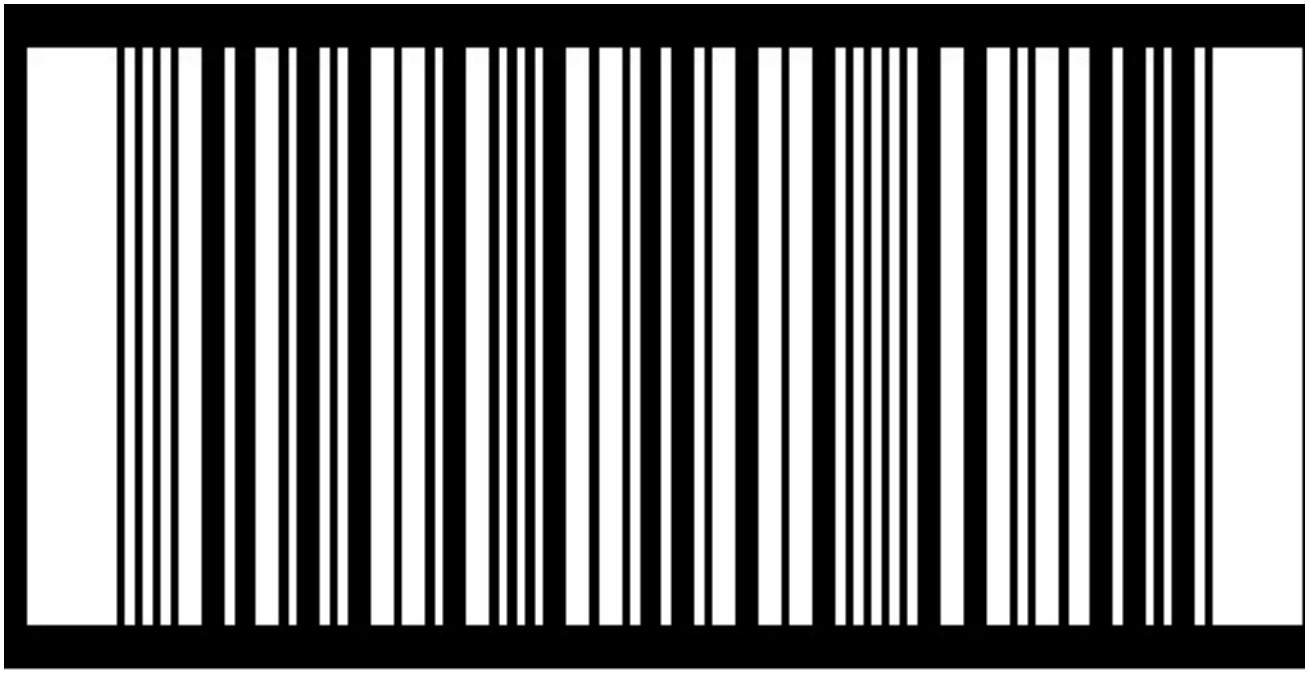
O criminoso faz contato através de uma ligação se passando por funcionário de site de compra e de um banco e informa que estará encaminhando um código promocional ou de confirmação.

Como evitar –

- ✓ Ative a confirmação em duas etapas do WhatsApp.
- ✓ Nunca forneça código verificador que receber por SMS no seu celular
- ✓ Não instale aplicativos de terceiros e não forneça suas informações pessoais a pedido de ninguém pelo WhatsApp.



BOLETO FALSO



O boleto bancário trata-se de um documento com um código de barras onde o beneficiário receberá em sua conta um determinado valor, referente a um produto ou serviço.

O criminoso utilizando engenharia social e ou através de um link fraudulento, altera o código de barras colocando como beneficiário outra conta bancária.

Este crime já foi muito utilizado contra empresas/corporações onde, falsificavam contas comuns, pagamentos diversos e contas dos cartões corporativos dos executivos. Para isso havia participação de funcionários do condomínio/prédio.

BOLETO BANCÁRIO

Como Evitar –

- Verifique se os dados do “beneficiário” correspondem aos que lhe vendeu o produto e ou serviço
- Confira se os três primeiros números do código de barras correspondem ao banco cujo a logomarca aparece no boleto
- Desconfie se o código de barras estiver com falhas que apresentem espaços excessivos entre as barras ou qualquer outra alteração que impossibilite o reconhecimento pela leitora.

SEXTORSÃO

Consiste em ameaçar alguém (vítima) que irá disponibilizar ao público imagens e ou vídeos íntimos e neste caso, pode ocorrer por vingança, humilhação ou para ter uma vantagem financeira.

A vítima em questão, pode ter compartilhado uma imagem por impulso, pode ter tido um relacionamento com o agressor e ou apenas acredita que ele possua estas imagens/vídeos.

Ocorre que, ao ser ameaçado, a vítima pode ter uma incerteza se em algum momento compartilhou ou não imagens íntimas e esta situação será favorável ao crime de extorsão.

SEXTORSÃO - COMO EVITAR

- Evite compartilhar fotos e vídeos íntimos.
- Desconfie de pedidos de amizades de desconhecidos.
- Evite participar de chamadas de vídeos com desconhecidos, o perfil e a imagem do outro lado pode ser falsa.
- Evite manter fotos íntimas no celular, pois ele pode ser roubado/furtado e ou você poderá que mandar ele para um reparo e terão acesso ao conteúdo do seu celular.
- Tenha sempre um antivírus instalado nos seus equipamentos.

GOLPE DO FALSO LEILÃO E OU FALSO EMPRÉSTIMO

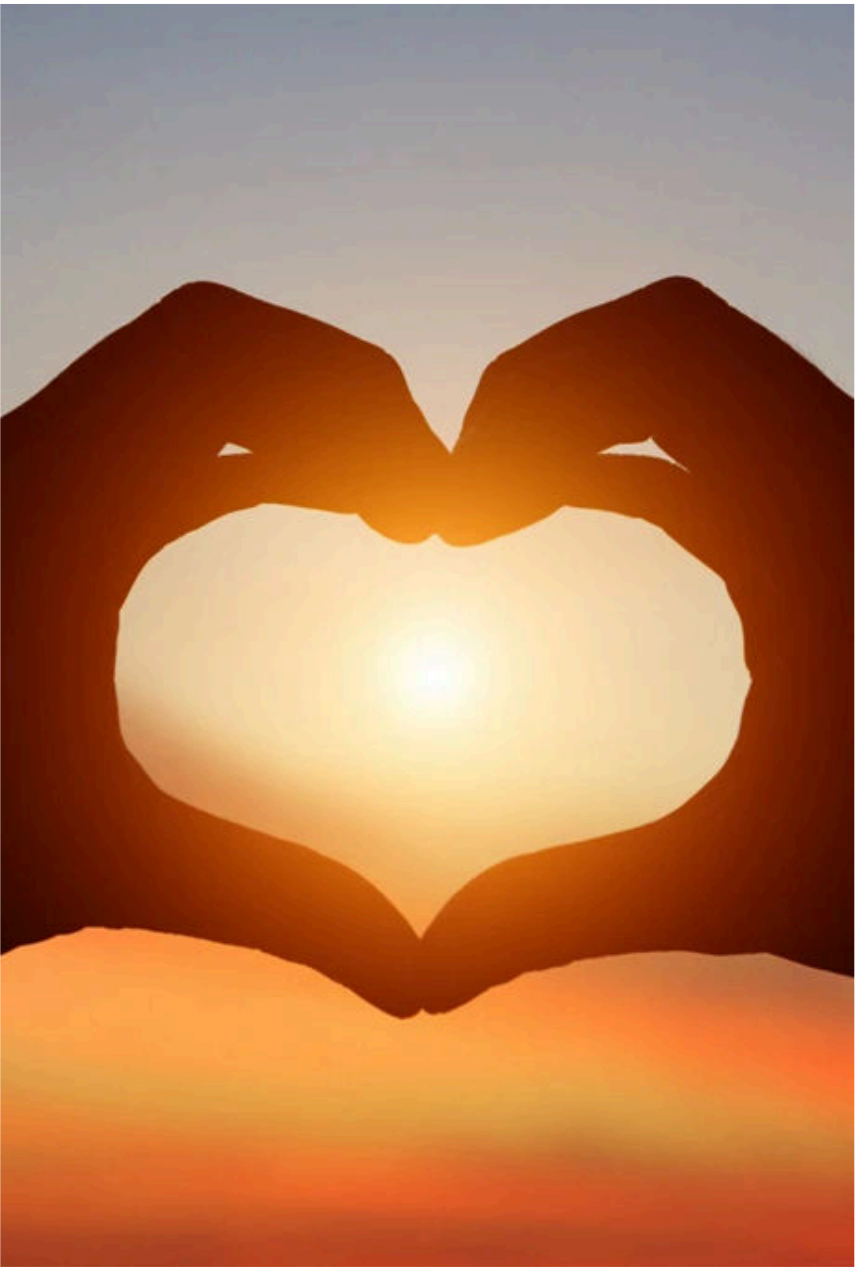
O golpe do falso leilão é praticado pela internet onde, o crimino cria um site falso, contendo fotografias de veículos para simular um leilão online. Após a vítima efetuar um lance recebe a informação de que venceu o leilão e recebe um termo de arrematação, contendo instruções para retirada do veículo e sobre o pagamento. Geralmente após a transferência inicial para a conta indicada, a vítima não consegue mais contato com a empresa. Em alguns casos, devido ao grande número de vítimas, a empresa ainda opera e fornece informações por dias.

GOLPE DO FALSO LEILÃO

Como evitar –

- Procure utilizar terminais seguros (Notebooks, Smartphone e Tlabet) que sejam seguros.
- Lei atentamente as informações contidas no site e do veículo que deseja arrematar, é comum que sites fraudulentos contenham erros de português e nas especificações técnicas.
- Pesquise o CNPJ e do endereço informado no site.
- Faça uma pesquisa na internet para obter informações a respeito da reputação do site.
- Verifique que o site é seguro, localizando o ícone de um cadeado, ao lado do endereço do site (URL). Ao clicar no cadeado será exibido o certificado de segurança da página.
- Evite clicar em links que irão te direcionar diretamente ao site do leilão online. De preferência em digitar o endereço do site (URL) na barra de endereço do seu navegador.

É comum que os criminosos criem/utilizem páginas muito similares as dos leiloeiros oficiais.



GOLPE DO AMOR – GOLPE DON JUAN

Hoje mais do que nunca e ainda, com a pandemia, houve um aumento considerável da busca de plataformas digitais de relacionamentos.

Já em contrapartida, criminosos criam perfis falsos para se aproximar de vítimas e através de juras de amor e outras promessas, conseguem obter a confiança necessária para aplicar o golpe.

Após criar uma enorme expectativa de um relacionamento envolvendo amor, o criminoso utiliza esta confiança para obter vantagens financeiras. As histórias podem ser a mais variáveis, como empréstimo para poder ter o encontro pessoal, depósito para retirada de presentes enviados por correios e muitos outros.

GOLPE DO AMOR – GOLPE DON JUAN
COMO EVITAR

- Dialogue com parentes e amigos (que tenha confiança) sobre seu relacionamento e peça opinião deles sobre qualquer pedido de valor monetário.
- Procure marcar encontros em locais públicos e que você conheça.
- Desconfie da solicitação de valores, sejam estes quais forem e procure obter mais informações sobre esta pessoa.
- Não forneça informações pessoais relevantes como local de trabalho, renda, com quem mora e seu endereço se não tiver plena confiança em que está do outro lado.

RANSOMWARE – SEQUESTRO/CAPTURA DE DADOS

De uma forma simplista, podemos classificar o Ransomware como um vírus que trava/tranca seus dados até que haja um pagamento de resgate.

O criminoso através de artifícios consegue invadir o computador e ou rede da vítima e instala um software que criptografa (codifica) o computador e/ou uma rede corporativa da vítima.

Recentemente tivemos muitos casos de Corporações no Brasil que foram vítimas destes criminosos e muitas delas pagaram altos resgates para voltar a operar.

Por Exemplo -

“O frigorífico JBS confirmou ao The Wall Street Journal, que pagou 11 milhões de dólares aos hackers que atacaram os sistemas da empresa no Estados Unidos e na Austrália no final de maio de 2021”.

RANSOMWARE – SEQUESTRO/CAPTURA DE DADOS

As empresas de manufatura têm sido as vítimas preferenciais deste tipo de crime. Em 25% dos casos, são elas os alvos. Só depois que aparecem os setor de serviços e os diversos órgãos dos governos. São organizações/empresas que, em caso de elevado tempo de inatividade das operações podem perder milhões de dólares por dia.

A IBM calcula que a **Sodinokibi**, também conhecido como REvil, esteve à frente de pelo menos 140 ataques a organizações desde seu surgimento em abril de 2019.

Até hoje, o menor valor solicitado foi de US$ 1,5 mil, enquanto o maior atingiu a marca de US$ 42 milhões. “Uma estimativa conservadora para os lucros do ransomware Sodinokibi em 2020 é de pelo menos US$ 81 milhões”.

FONTE – Olhar Digital e IBM (05/10/2020)

SITES DE COMÉRCIO ELETRÔNICO FRAUDULENTOS

O criminoso cria uma página na internet muito similar a verdadeira e leva a vítima a acreditar que está efetuando uma compra legítima.

Normalmente a vítima seleciona o produto e efetua a compra, todavia, não recebe a mercadoria e neste momento, percebe que caiu em um golpe.

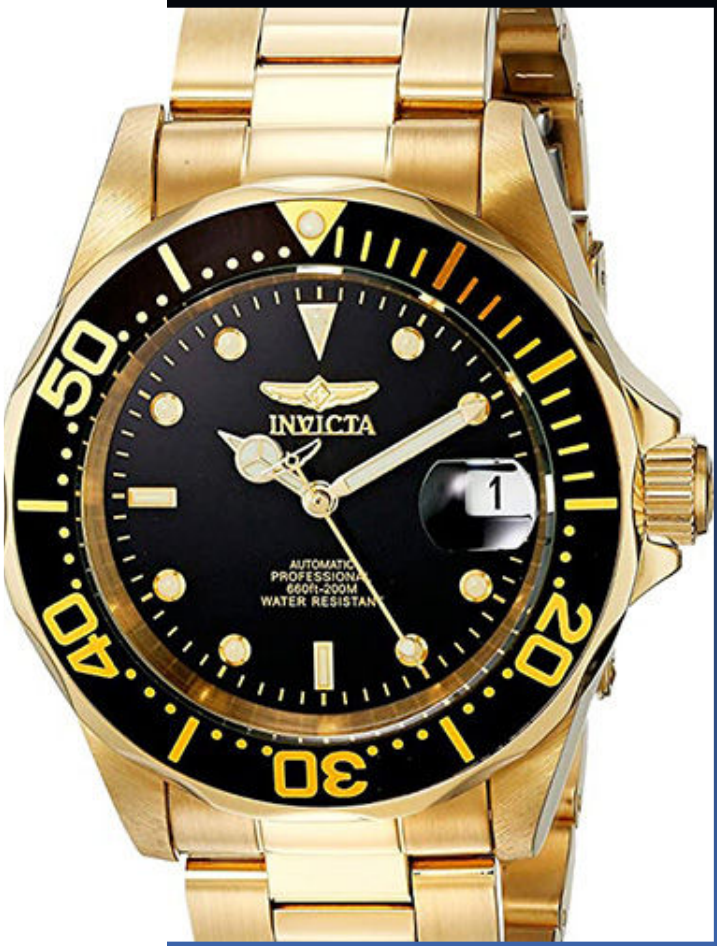
Para aumentar a chance de sucesso o criminoso envia spam e ofertas com produtos com valores abaixo do valor de mercado e links patrocinados.

No mês de novembro quando há Black Friday esta modalidade de crime tem um aumento considerável.

SITES DE COMÉRCIO ELETRÔNICO FRAUDULENTOS

Como evitar –

- Faça uma pesquisa de mercado do valor do produto.
- Leia atentamente as informações do produto e do site, normalmente sites falsos podem conter erros de português e ou erros sobre as informações técnicas do produto.
- Faça pesquisas na internet sobre a reputação do site que pretende comprar. Você poderá obter estas informações através de redes sociais ou do site reclame Aqui.
- Desconfie de preços muito baixos e vantagens absurdas.



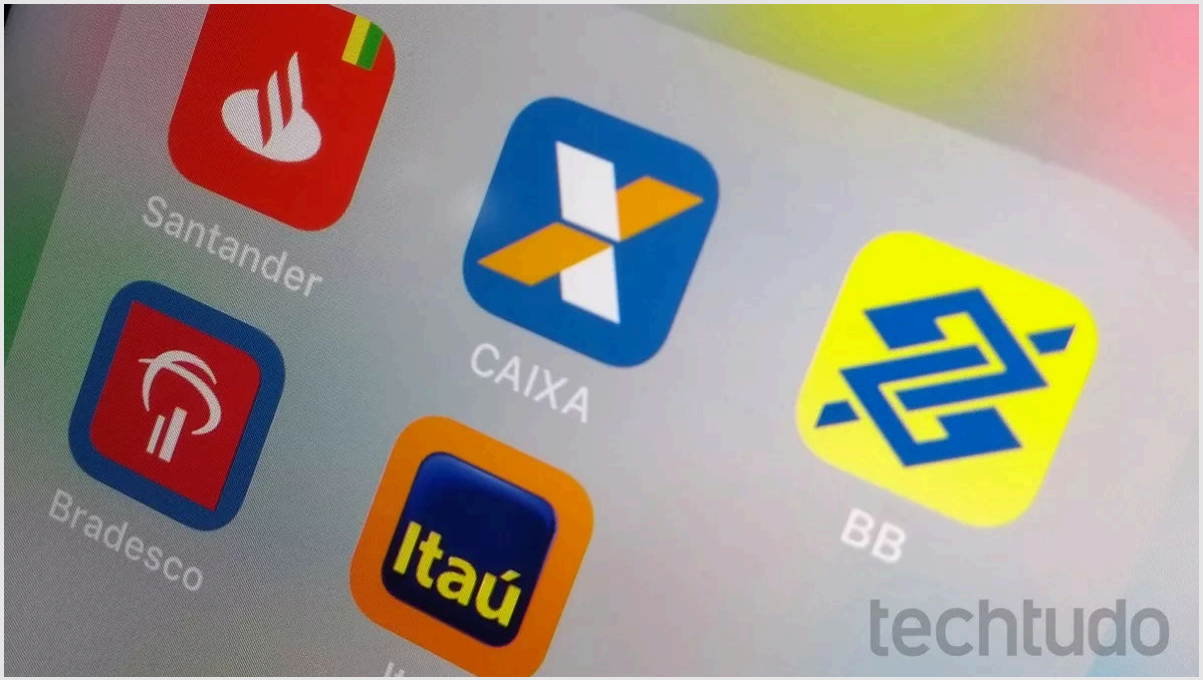
GOLPES ENVOLVENDO PIX

Quando pensamos nos cuidados que devemos ter com o PIX, devemos considerar os mesmos cuidados que temos os outros serviços financeiros já utilizados como TED e DOC.

Ocorre que, a agilidade de realizar um PIX fez com que os criminosos quando do cometimento de crimes de roubo, já obriguem suas vítimas a realizar PIX em contas de terceiros (laranjas).

Os SmartPhones em geral nos proporcionam facilidades em relação aos acessos aos bancos e ao serviço do PIX e esta facilidade é muito bem utilizada por criminosos.

GOLPES ENVOLVENDO PIX



O serviço de PIX veio para atender as necessidades atuais de pagamentos e facilidade aos usuários más, em contrapartida, nos deixa vulneráveis se estivermos sobre a guarda de criminosos que poderão exigir que façamos pagamentos e transferências contra nossa vontade.

Não há grandes soluções onde se possa evitar ser obrigado a realizar estas transferências umas vez que estivermos sobre o controle de criminosos.

Más, podemos tomar algumas ações que irão minimizar nossos riscos.

GOLPES ENVOLVENDO PIX

CUIDADOS QUE DEVEMOS TOMAR

- Saiba, não existe sites do banco Central ou do PIX para cadastramentos de chaves, nem para realização de transações com PIX.
- Todos cadastramentos são feitos quando você está logado no ambiente do seu banco de relacionamento.

RECOMENDAÇÃO – Nunca negocie e ou discuta com o criminoso, nada tem mais valor que sua integridade física, sua vida.

GOLPES ENVOLVENDO PIX

AÇÕES QUE DEVEMOS TOMAR –

- Não deixe o símbolo do aplicativo do seu banco na tela inicial do seu SmartPhone, busque sempre deixa-lo de forma mais oculta possível.
- Busque Apps que possibilitem a ocultação do ícone do seu banco.
- Coloque limites junto ao seu banco em suas transações com PIX.

MUITO OBRIGADO A TODOS

Perguntas, estamos sempre a disposição

iangelo@afimacglobal.com
www.afimacglobal.com

Fim da Apresentação