ESTELIONATO E FRAUDE NO ÂMBITO CIBERNÉTICO

O USO DE SOFTWARES MALICIOSOS NA PRÁTICA DE CRIMES VIRTUAIS

OS CUIDADOS QUE OS CONSUMIDORES DEVEM TER NA HORA DE COMPRAR ONLINE.

A presente pesquisa irá retratar os perigos e ameaças que o consumidor do âmbito digital está refém, como por exemplo o crime de estelionato e fraude. Salientaremos os riscos que há quando nós, consumidores, deixamos nossos dados em sites de compras, como por exemplo, CPF, endereço e até mesmo dados do cartão de crédito.

Alunos: Adryelle Cossuol, Bruna Lima, Kamila Lifonsa, Lucas Ohnesorge, Relberth Martins e Samira Lipaus
5º período da Faculdade Multvix.

MAS AFINAL DE CONTAS, QUAIS AS DEFINIÇÕES DE ESTELIONATO E FRAUDE?

NÃO SABE?! **KEEP CALM** IREMOS TE EXPLICAR**.**

O crime de estelionato está previsto no art. 171 do CP, é uma infração penal muito comum,
que exige quatro requisitos, obrigatórios para sua caracterização:

1) obtenção de vantagem ilícita;
2) causar prejuízo a outra pessoa; ;
3) uso de meio de ardil, ou artimanha,
4) enganar alguém ou a leva-lo a erro.

Desta forma, tem-se que o estelionato acontece quando uma pessoa usa o engano ou a **fraude** para levar vantagem sobre alguém.

Ainda está com dúvidas? Vamos te daremos um exemplo: Maria compra pela Internet um lindo e luxuoso colar de ouro e recebe, em seu lugar, uma bijuteria (de forma proposital), isso caracterizar o crime de estelionato.

Mas qual é o conceito de fraude?
Em direito penal, fraude é o crime ou ofensa de deliberadamente **enganar** outros com o propósito de prejudicá-los, usualmente para obter propriedade ou serviços dele ou dela injustamente.
A fraude e o estelionato são melhores amigos, andam lado a lado, tendo em vista que para ocorrer o crime disposto no art. 171 do CP, é necessário a utilização do meio fraudulento e enganoso, para obter vantagem ou favorecimento da vítima.

Tendo conhecimento nos conceitos dos crimes que abordamos, podemos então seguir para um assunto muito relevante, **os malwares.**

O termo malware diz respeito a um software malicioso utilizados com diferentes objetivos; danificar dispositivos, rouba dados, causa algum tipo de dano em sua essência.

Nesta perspectiva, sabe-se da existência vários tipos de malwares, como vírus, cavalo de troia, spyware, ransomware, adware, hijacker, etc., Contudo existe condutas e ferramentas de combate a eles, visando um ambiente mais seguro, adotando, por exemplo, o uso de Antimalwares, aplicativos de Antivirus e atitudes como a não execução de arquivos desconhecidos, ou a desabilitacão da execução automática, entre outras.

CRACKER & HACKER

Geralmente, um malware é desenvolvido por pessoas com um vasto conhecimento na área da informática. Entretanto, cumpre enfatizar os dois principais tipos de pessoas com tal conhecimento, CRACKER e HACKER.

Geralmente, um malware é desenvolvido por CRACKER, sendo a principal característica desse tipo de pessoa, utilizar tais conhecimentos para fins maliciosos. Buscando uma forma de fazer dinheiro, seja pela proliferação do próprio malware ou por meio de leilão na Dark Web. De qualquer forma, podem haver outras razões para a criação de malwares.

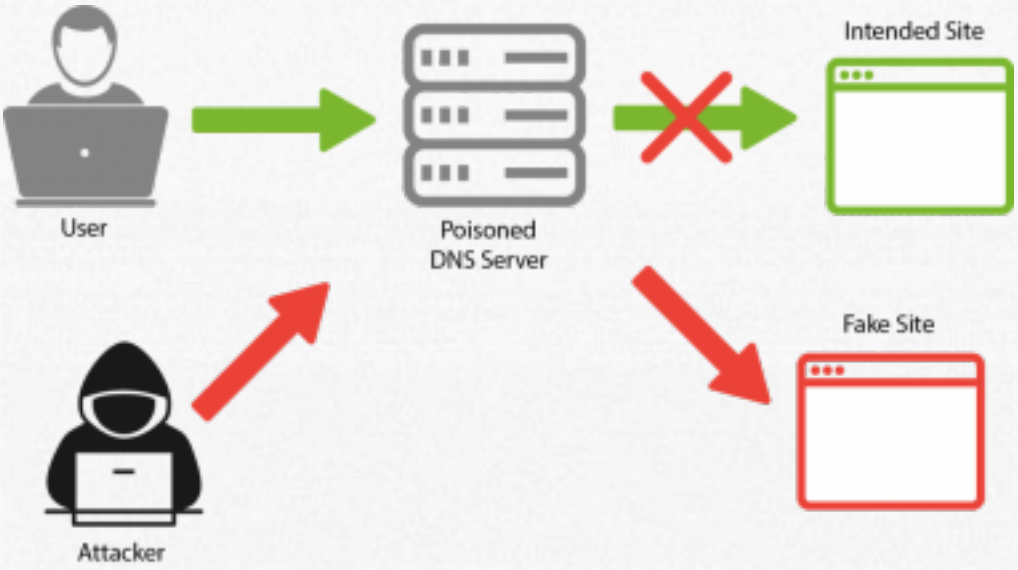
Diferentemente do HACKER, que na maioria das vezes é um indivíduo contratado por empresas a fim de testar a segurança dos teus sites ou até mesmo criando dispositivos para aumentar a segurança do respectivo ambiente virtual.

- **PRINCIPAIS PROGRAMAS MALICIOSOS ATUALMENTE**

HIJACKER: A Fraude da página falsa para extrair dados, que consiste em uma reprodução quase idêntica da página, porém, com diferenças minúsculas e quase imperceptíveis no endereço de acesso a página.

O supracitado software malicioso é popularmente conhecido como HIJACKER "Página Falsa", sua função principal diz respeito ao sequestro de navegadores, ou seja, ele captura o browser original fixando uma página idêntica às originais visando tomar conhecimento de dados inseridos nesta página falsa.

Geralmente, tal programa malicioso é usado em sites de bancos ou até mesmo em lojas virtuais, com o objetivo de passar a ter conhecimento de cartões de crédito ou até mesmo acesso a contas pessoais bancárias. Com isso, os criminosos se encontram aptos a realizar compras utilizando os dados do consumidor, que na maioria das vezes descobrem tardiamente que foram enganados por criminosos, gerando em seu cartão compras sem a sua anuência de forma descontrolada.



ADWARE

É importante salientar que esse programa corresponde como sendo um SPYWARE, ou seja, um tipo de malware espião. No entanto, curiosamente se pode afirmar que existe a possibilidade de usá-lo de forma benéfica, como em ambientes de relação empregatício.

Contudo, geralmente é um tipo de spyware destinado a capturar informações de pesquisa repassando essas pesquisas a empresas. Como exemplo, pode citar o fato de um usuário pesquisando um tênis, mas não o compra. Logo em seguida, em seu navegador aparece várias propagandas a respeito da pesquisa realizada.

Esse programa tem uma ligação direta com o hijacker, calcado no fato de que o adware pode ser usado como ferramenta para capturar dados pessoais, transferindo o usuário a uma possível página falsa e a partir dali, cometer crimes virtuais.

FIQUE ATENTO AO UTILIZAR REDES DE INTERNET EM AMBIENTES PÚBLICOS

Quando você está no shopping, prestes a fazer uma compra, pode ser interessante fazer uma última comparação com as melhores ofertas oferecidas pelas lojas virtuais. Entretanto, existem vários riscos à segurança se você acessar a Internet por uma rede Wi-Fi pública.

Os criminosos virtuais podem interceptar seus dados e capturar suas senhas, detalhes de login e informações financeiras. Se precisar acessar a Internet enquanto faz compras, use a rede do celular. Portanto, jamais faça o login, ou cadastre cartões de crédito usando uma rede pública. A possibilidade da existência de um SPYWARE, software malicioso espião, é absurdamente grande.

MANTENHA O ANTIVÍRUS ATUALIZADO

Os denominados CRACKER, pessoas que têm um vasto conhecimento na informática e a utilizam para a prática de crimes virtuais, constantemente criam novos softwares maliciosos almejando driblar os aplicativos de combate a esses malwares. Desta forma, é fundamental manter atualizado o antivírus a fim de que identifique novas assinaturas danosas.

No que diz respeito aos vírus, a grosso modo, sabe-se que são assinaturas, códigos, por isso a importância de manter o antivírus atualizado, pois ele incluirá em seu combate novas assinaturas, novos códigos correspondente aos programas maliciosos.

FAÇA PESQUISA DE FORMA MAIS SEGURA NA INTERNET

Embora os mecanismos de pesquisa sejam úteis para procurar produtos, avaliações ou fazer comparações de preços, você corre sempre o risco ao navegar pela internet. Isso é afirmado amparado pelo fato que a internet se trata de uma rede pública, trata-se de uma rede mundial onde a segurança de forma absoluta é considerada uma utopia.

Assim, sempre existe a possibilidade, mesmo que mínima ou até mesmo sem querer, de executar arquivos ou abrir portas que geram resultados "envenenados", que podem abrir caminhos para programas maliciosos e não ao destino pretendido. Os resultados de pesquisa envenenados são criados por criminosos virtuais que usam truques de otimização do mecanismo de pesquisa (SEO), muitas vezes chamados de Black SEO, para manipular os resultados e incluir links maliciosos.

Atente-se a protocolos como o HTTPS, tal protocolo promove um ambiente mais seguro, pois carrega consigo o uso da criptografia.

Em vez de simplesmente clicar em um link para chegar ao site da loja desejada, é mais seguro digitar o URL da loja na barra de endereços do navegador da Web. Pode demorar um pouco mais, mas essa ação tão simples pode evitar que você acesse um site falso ou malicioso.

GERENCIE E PROTEJA SUAS SENHAS

Usar um gerenciador de senhas pode ajudar a lidar com diversas contas e senhas, além de criptografar as senhas que, de outra forma, estariam em texto simples. Atualmente existem inúmeras formas de elaborar uma senha, sendo exigido inclusive determinados caracteres. É encontrado até mesmo o uso de estrutura óssea do rosto dos usuários para que seja promovida a maior segurança possível da informação.