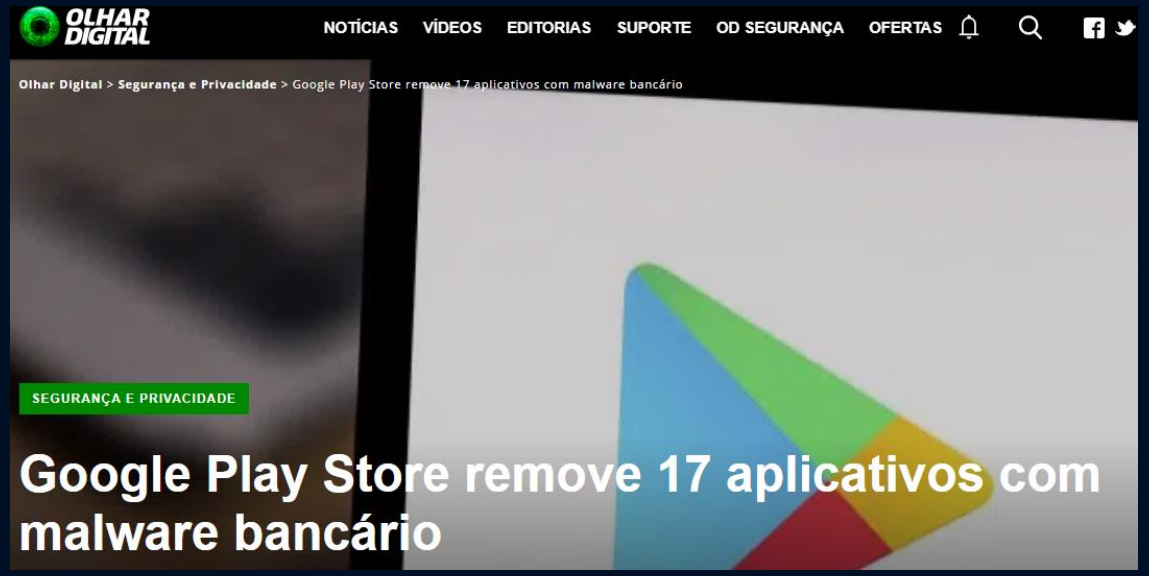
Instituto Infnet

Segurança da Informação

FABIANO GISBERT

ETAPA 02

https://olhardigital.com.br/2022/07/27/seguranca/aplicativos-maliciosos-android/amp/



https://olhardigital.com.br/2022/08/02/seguranca/google-play-store-remove-17-aplicativos-malware-bancari/

https://canaltech.com.br/seguranca/criminosos-tem-novas-taticas-para-roubar-dados-de-cartao-de-credito-217199/

Segurança da Informação

Instituto Infnet

Incidentes x Ataques

Ambos derivam de um risco não tratado, porém os incidentes de segurança são genéricos e podem agir de forma intencional ou de forma acidental, podem ser internas ou externas, e podem ser previsíveis ou imprevisíveis, como incêndios, enchentes, terremotos, guerra, etc.

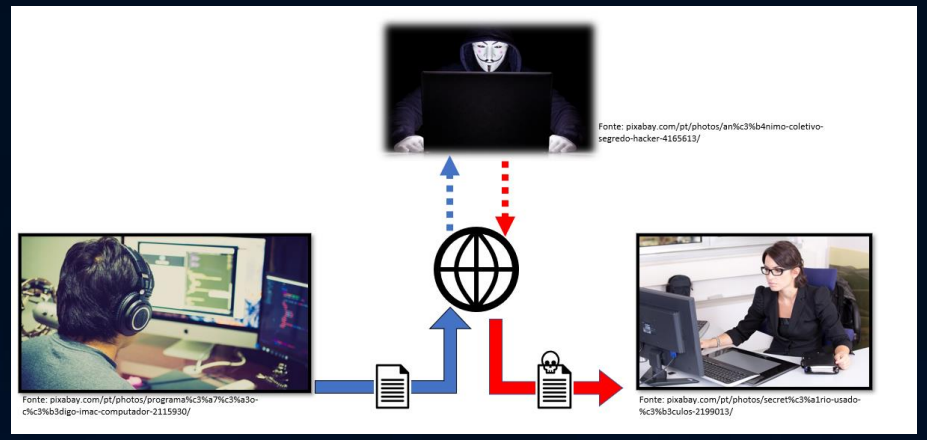
Já o Ataque deriva de uma ameaça conduzida, ou seja, um ato deliberado (especialmente no sentido de um método ou técnica) de violar a política de segurança de um sistema e obter acesso à uma informação sigilosa ou deixa-la indisponível.

Segurança da Informação

Instituto Infnet

Tipos de Ataques - ATIVOS

Os Ataques ativos são aqueles onde são perceptíveis à vítima tão logo ele ocorra. Neste tipo, o atacante é capaz de interceptar e alterar os dados transmitidos, utilizando para isso desde a falsificação de dados, nos mais diversos níveis.



Segurança da Informação

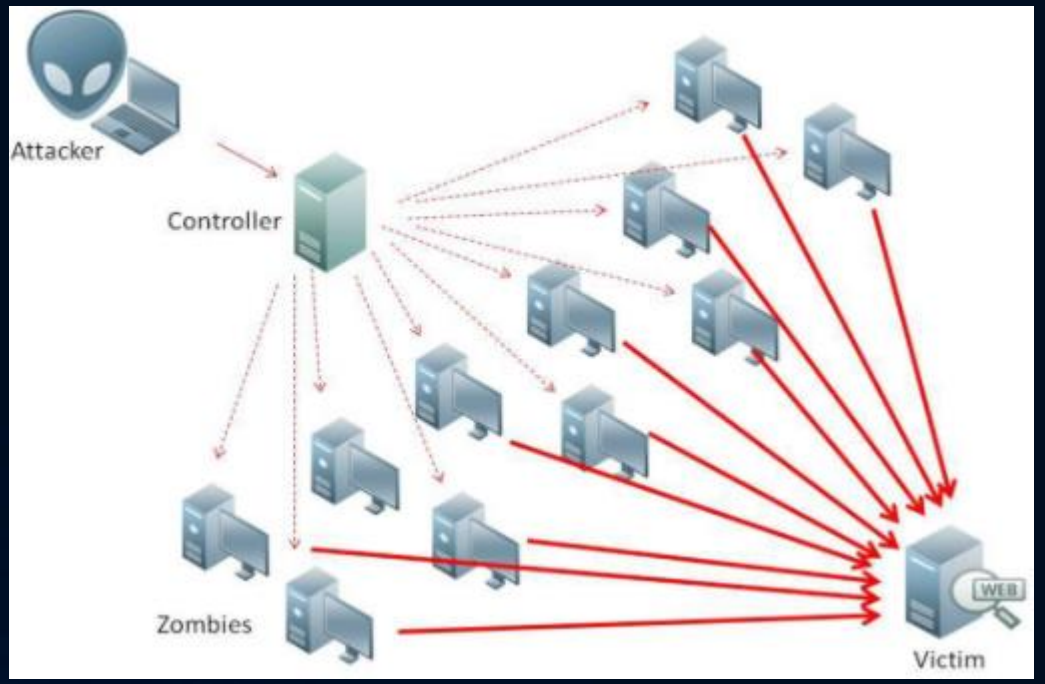
Instituto Infnet

Tipos de Ataques – ATIVOS (Exemplos)

Denial of Service (DoS)

Um ataque de negação de serviço (DoS) é um tipo de ataque cibernético em que um ator malicioso tem por objetivo tornar um computador ou outro dispositivo indisponível para os usuários a que se destinam, interrompendo o funcionamento normal do dispositivo.

Os ataques DoS normalmente funcionam sobrecarregando ou inundando uma máquina visada com solicitações até que o tráfego normal não possa ser processado, resultando em negação de serviço para usuários adicionais. Um ataque DoS caracteriza-se pelo uso de um único computador para lançar o ataque.



Segurança da Informação

Instituto Infnet

Tipos de Ataques – ATIVOS (Exemplos)

Malwares

VÍRUS

O vírus de computador é o que as pessoas popularmente chamam de malware, mas há uma diferença entre as duas aplicações: todo vírus de computador é um malware, mas nem todo malware é um vírus.

Este último é uma forma de aplicação maliciosa que modifica outros arquivos host legítimos de modo que, quando o arquivo infectado é executado, o vírus também é executado.

Assim, pode atrapalhar ou inviabilizar a realização de tarefas, propagando-se sem ação do usuário.

Segurança da Informação

Instituto Infnet

Tipos de Ataques – ATIVOS (Exemplos)

Malwares

VÍRUS

```
seg000:00000DD0 20 20 48 54 54 50+aHttp1_0Content db ' HTTP/1.0',0Dh,0Ah
seg000:00000DD0 2F 31 2E 30 0D 0A+ db 'Content-type: text/xml',0Ah
seg000:00000DD0 43 6F 6E 74 65 6E+ db 'HOST:www.worm.com',0Ah
seg000:00000DD0 74 2D 74 79 70 65+ db ' Accept: */*',0Ah
seg000:00000DD0 3A 20 74 65 78 74+ db 'Content-length: 3569 ',0Dh,0Ah
seg000:00000DD0 2F 78 6D 6C 0A 48+ db 0Dh,0Ah,0
seg000:00000E2C 63 3A 5C 6E 6F 74+aCNotworm db 'c:\notworm',0
seg000:00000E37 4C 4D 54 48 0D 0A+aLmthHtmlHeadMe db 'LMTH',0Dh,0Ah
seg000:00000E37 3C 68 74 6D 6C 3E+ db '
seg000:00000E37 3C 6D 65 74 61 20+ db 'ize=5>
Welcome to http://'
seg000:00000E37 68 74 74 70 2D 65+ db 'www.worm.com !

Hacked By Chinese!<'
seg000:00000E37 71 75 69 76 3D 22+ db '/html> '
seg000:00000E37 43 6F 6E 74 65 6E+ db ' '
seg000:00000E37 74 2D 54 79 70 65+ db ' '
seg000:00000E37 22 20 63 6F 6E 74+seg000 ends
seg000:00000E37 65 6E 74 3D 22 74+
seg000:00000E37 65 78 74 2F 68 74+
seg000:00000E37 6D 6C 3B 20 63 68+ end
```

Segurança da Informação

Instituto Infnet

Tipos de Ataques – ATIVOS (Exemplos)

Malwares

CAVALO DE TROIA (TROJAN)

O Cavalo de Troia, ou Trojan, é uma das formas mais perigosas, pois geralmente se apresentam como um programa útil de modo a enganar o usuário.

Na maioria das vezes, chegam por e-mail ou são encaminhados aos usuários que visitam sites infectados.

Assim, conseguem enganar as pessoas e evitar formas de defesa tradicionais, como firewall e antivírus, por exemplo.

Uma vez que está instalado no sistema, os invasores que criaram o Trojan têm acesso ao dispositivo afetado e podem instalar outras ameaças mais graves ou até mesmo roubar informações financeiras.

Segurança da Informação

Instituto Infnet

Tipos de Ataques – ATIVOS (Exemplos)

Malwares

RANSOMWARE

O Ransomware é um tipo de malware que criptografa os arquivos e/ou bloqueia o dispositivo infectado, mantendo os dados como reféns até o pagamento de um resgate, geralmente por meio de uma criptomoeda.

Em muitos casos, o malware é distribuído por algum tipo de engenharia social, ou seja, os usuários entram em um site malicioso ou instalam um programa mal-intencionado sem saber.

Ao ser executada, a aplicação pode criptografar os arquivos em poucos minutos ou até mesmo observar a rotina do usuário para identificar outros backups supostamente seguros.

Segurança da Informação

Instituto Infnet

Tipos de Ataques – ATIVOS (Exemplos)

Ataque de Perímetro

Cross-site scripting (XSS)

Ataques de cross-site scripting envolvem código malicioso sendo injetado em sites de outra forma confiáveis. Um ataque de cross-site scripting ocorre quando os criminosos cibernéticos injetam scripts maliciosos no conteúdo do site alvo, que é então incluído com o conteúdo dinâmico entregue ao navegador da vítima. O navegador da vítima não tem como saber que os scripts maliciosos não são confiáveis e, portanto, os executa.

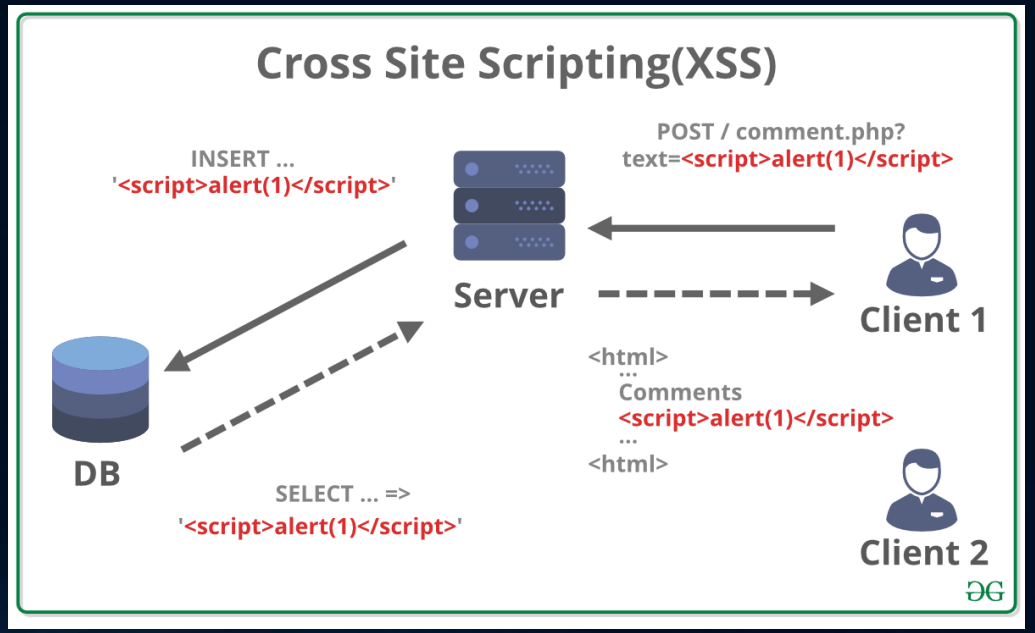
Como resultado, os scripts maliciosos podem acessar quaisquer cookies, tokens de sessão ou outras informações confidenciais retidas pelo navegador e usadas nesse site. Os invasores também podem usar XSS para espalhar malware, reescrever o conteúdo de sites, causar problemas em redes sociais e phishing para credenciais de usuário

Segurança da Informação

Tipos de Ataques – ATIVOS (Exemplos)

Ataque de Perímetro

Cross-site scripting (XSS)



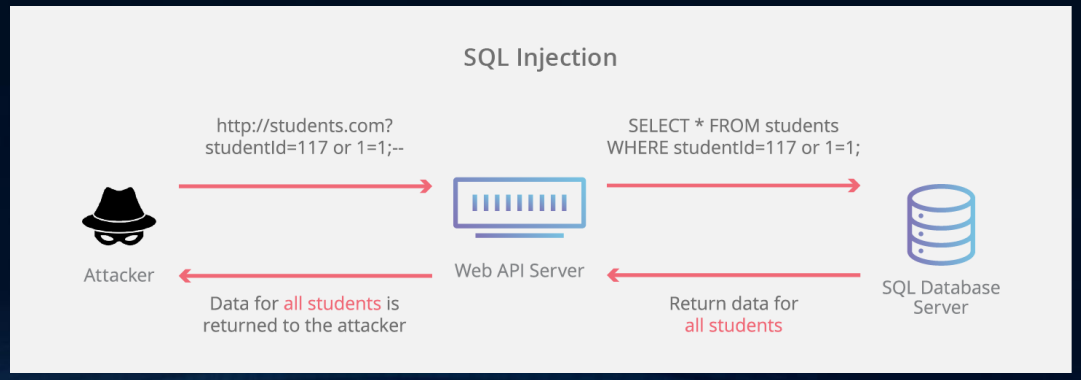
Segurança da Informação

Tipos de Ataques – ATIVOS (Exemplos)

Ataque de Perímetro

SQL Injection

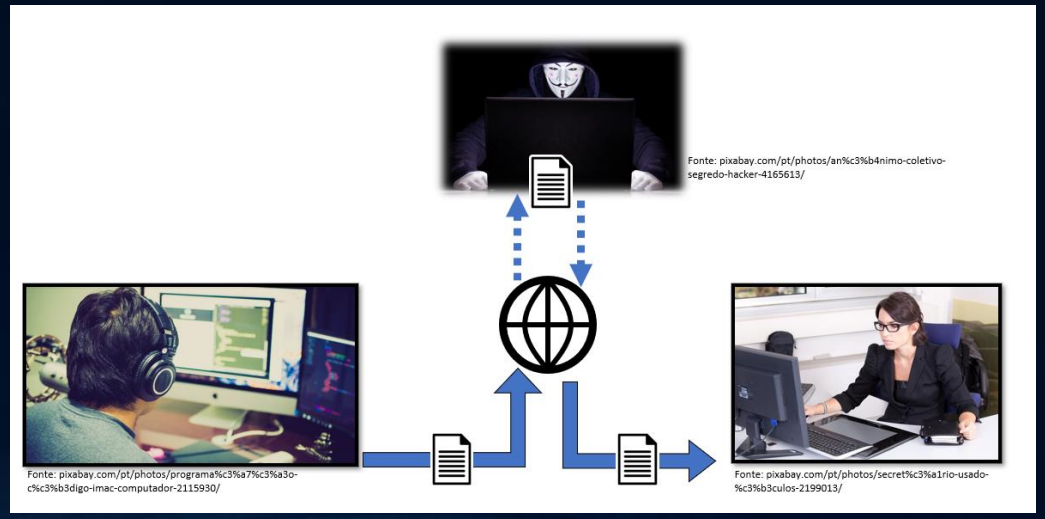
Uma injeção de SQL, às vezes abreviada como SQLi, é um tipo de vulnerabilidade em que um invasor usa uma parte do código SQL (Structured Query Language) para manipular um banco de dados e obter acesso a informações potencialmente valiosas. Esse é um dos tipos de ataque mais comuns e perigosos porque pode ser usado contra qualquer aplicação de Web ou site que utilize um banco de dados SQL (ou seja, a maioria deles).



Segurança da Informação

Tipos de Ataques – PASSIVOS

Neste tipo de ataque, o invasor não almeja danificar ou obstruir o acesso a informação, mas tão somente a capturá-las, usando alguma técnica, como as de escuta e captura de pacotes, ou através de métodos pessoais, como engenharia social.



https://g1.globo.com/pe/pernambuco/noticia/2022/08/25/criminosos-esvaziam-contas-bancarias-apos-invadir-celular-entenda-golpe-alvo-de-alerta-da-pf-e-saiba-como-se-proteger.ghtml

https://g1.globo.com/sp/sao-paulo/noticia/2022/09/09/25-moradores-de-sp-relatam-ter-caido-em-golpe-de-ingresso-para-rock-in-rio-era-pessoa-da-minha-rotina-nao-tinha-como-desconfiar.ghtml

Segurança da Informação

Instituto Infnet

Técnicas de Ataques PASSIVOS

- **Keylogger**: um programa criado para gravar tudo o que uma pessoa digita no teclado de um computador. Pode capturar senhas, dados bancários, informações sobre cartões de crédito e outros tipos de dados pessoais;
- **Impersonating**: uma variante de engenharia social, que consiste em ligar para uma pessoa se passando por outra e solicitar dados pessoais;
- **Phishing**: que consiste em mandar um email com link falso;
- **Tailgating**: que consiste em entrar em um local junto com outra pessoa;
- **Baiting**: que consiste em deixar algo de valor para a vítima, como um pendrive em cima da mesa, assim a pessoa fica curiosa, coloca no computador e infecta o sistema com um Keylogger, por exemplo
- **Backdoor**: A função de um backdoor é permitir algum tipo de acesso ilegal ao sistema alvo. Eles servem tanto para manter o acesso do atacante ao sistema invadido quanto para criar um novo canal de acesso.
- **Sniffers**: permite a captura de, entre outros dados, senhas de serviços inseguros como o Telnet, FTP e POP3. Eles são normalmente empregados pelo atacante para capturar dados trafegados numa rede que ele obteve acesso.

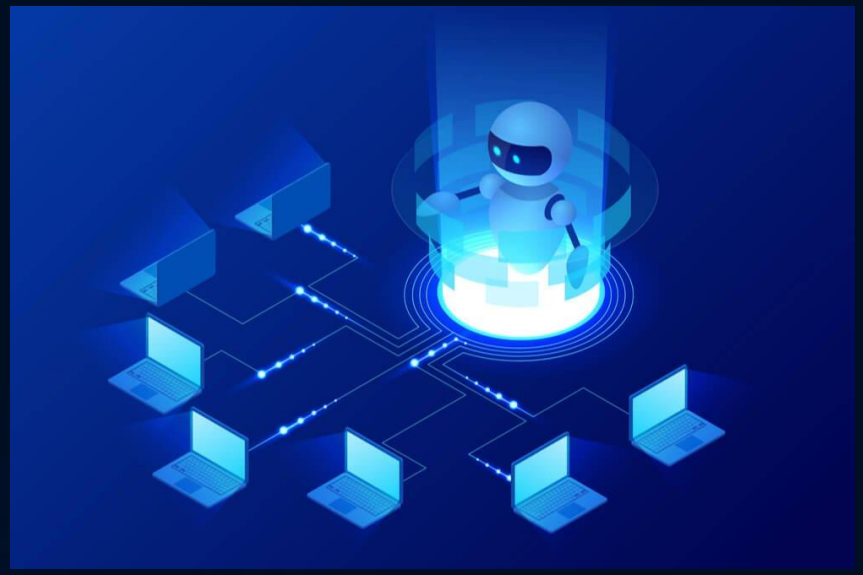
Ataques Passivos da Atualidade

Instituto Infnet

Bots

Um Bot (abreviação de “robô”, ou “robot” em inglês), é um tipo de script ou software que executa tarefas automatizadas de acordo com o comando. Muitos Bots são usados para executar tarefas maliciosas, permitindo que um invasor controle remotamente o dispositivo afetado.

As máquinas infectadas, também chamadas de zumbis, podem ser computadores ou dispositivos de IoT, por exemplo. Na maioria dos casos, os invasores coletam um grande número de computadores zumbi e os colocam em uma rede conectada, de modo que possam realizar atos danosos em grande escala.



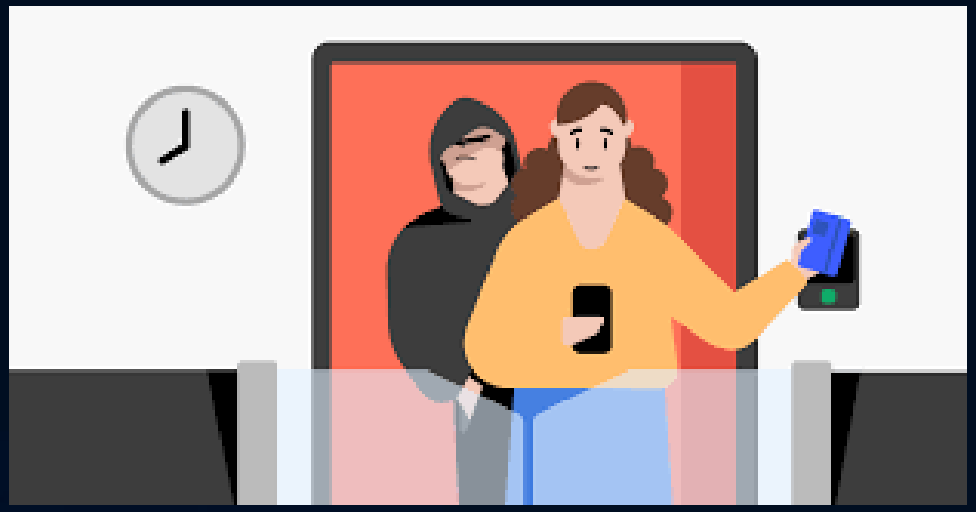
Ataques Passivos da Atualidade

Instituto Infnet

Tailgating

O tailgating na computação é uma prática recorrente da engenharia social e pode ser definido como um tipo de ataque onde o cibercriminoso segue um determinado usuário até alcançar dados sigilosos ou ambientes que provoquem erros propositais à rede.

Uma das técnicas mais comuns de tailgating é conseguir obter um crachá de acesso de visitante e entrar disfarçadamente em andares a qual não está autorizado seguindo o fluxo de funcionários do setor.



Ataques Passivos da Atualidade

Instituto Infnet

Engenharia Social:

Ao contrário da visão tradicional do hacker, um eremita digital, isolado em um porão escuro, sem contato humano, o engenheiro social é alguém que não estuda somente programação, mas também as relações humanas e a estrutura dos negócios.

A Engenharia Social trabalha com as falhas humanas no processo de segurança, então ela utiliza estatísticas de senhas mais comuns, vazamentos de informação, dados que fornecemos nas nossas redes sociais (nome da mãe, dos bichinhos de estimação, serviços que utilizamos) para conseguir acessar nossos dados.

Ataques Passivos da Atualidade

Instituto Infnet

Phishing

O aumento do número de pessoas conectadas à internet, por conta do isolamento social provocado pela pandemia do coronavírus, tem feito aumentar também a quantidade de golpes virtuais.

E um dos mais danosos entre todos é o Phishing, prática na qual pessoas mal intencionadas na Internet enganam as pessoas para que revelem informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Normalmente, eles fazem isso enviando e-mails ou mensagens de texto (SMS) direcionando os usuários a websites falsos

Ataques Passivos da Atualidade

Credential Stuffing:

É o ato de testar uma mesma credencial em múltiplos sites e sistemas para ver se o usuário a repetiu.

Com o aumento dos vazamentos de informações e uma maior quantidade de senhas para lembrar, nos levando a repeti-las, tornam o Credential Stuffing em um problema cada dia maior.

Ataques Passivos da Atualidade

Deep Fake:

O Deepfake se utiliza de técnicas de Deep learning para a criação de vídeos falsos (fake), daí que vem seu nome. Seu uso se tornou famoso quando vídeos falsos constrangedores de famosos e políticos apareceram na mídia.

Para se criar um deepfake é necessário acesso a vários vídeos de seu alvo, o que antes só era possível com pessoas famosas, agora, graças às mídias sociais, é possível criar com quase qualquer pessoa.

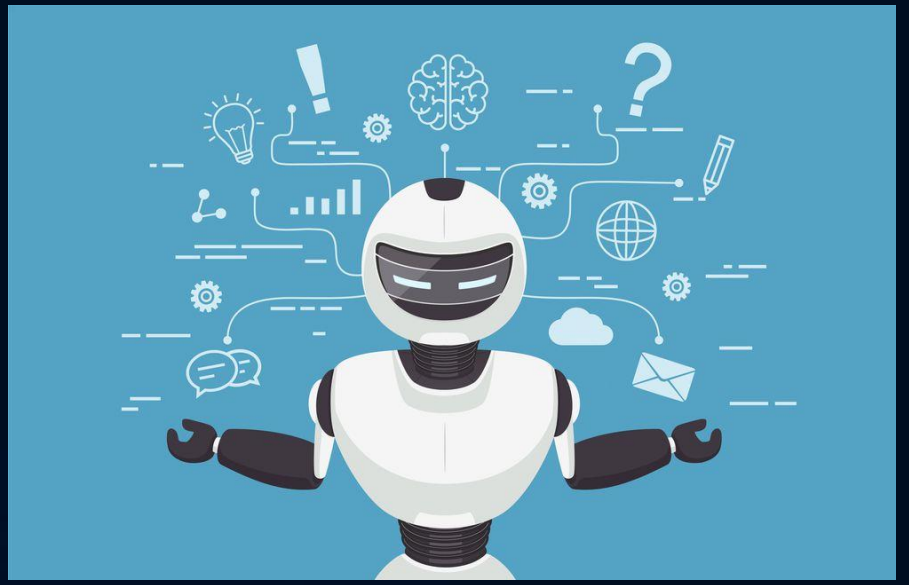
Principais Desafios Atuais

Instituto Infnet

Inteligência Artificial:

Se o uso de Inteligência Artificial tem aumentado no nosso dia-a-dia, pode ter certeza que hackers e outros fraudadores também estão utilizando. Hoje em dia as I.A. são utilizadas em quase todas as fraudes.

A inteligência artificial é fundamental para a criação de Deepfakes*, podem ser usadas em ataques de phishing e para quebrar os melhores sistemas de segurança. Entender em que pé está o desenvolvimento das Inteligências Artificiais é fundamental para a proteção de dados e outros tipos de ataques.

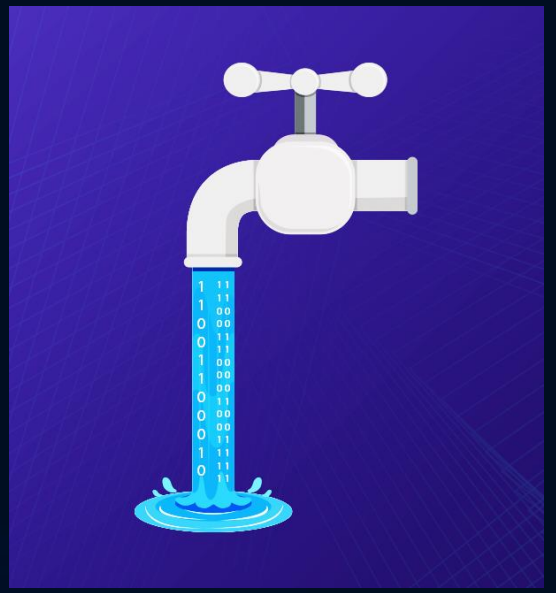


Principais Desafios Atuais

Vazamento de dados:

Desde a forma com que os dados são armazenados em mídia ou papel, até a forma como jogamos um documento fora, existem várias maneiras de expor informações.

Por isso, é sempre importante só armazenarmos ou manipularmos o mínimo de informações possível e sempre destruir qualquer documento que contenha informações sigilosas.

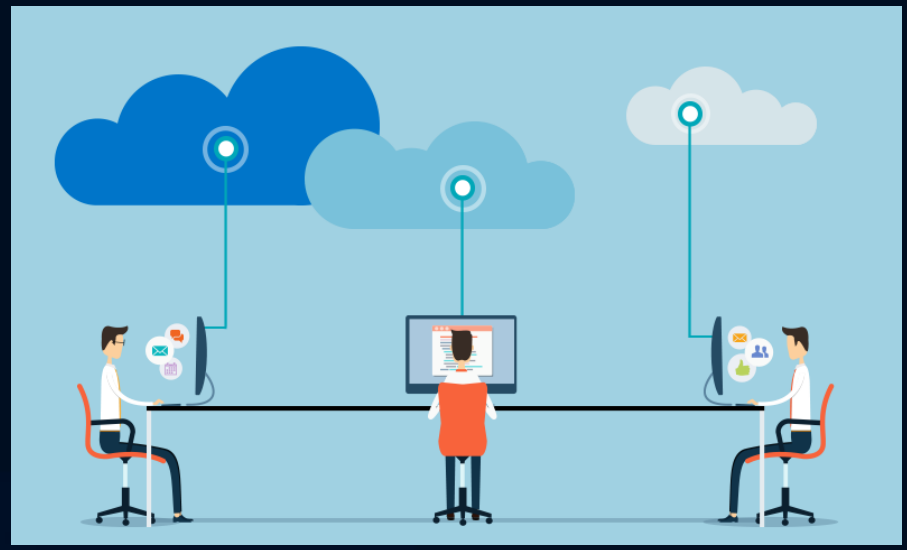


Desafios Atuais

Computação em Nuvem:

O uso de cloud computing tem crescido exponencialmente nos últimos anos.

O crescimento do cloud computing leva a uma questão importante: a visibilidade e atenção dos cibercriminosos, que veem oportunidades para obtenção de dados para fraudes bancárias, sequestros de dados, entre outros pontos que merecem atenção. Por isso, os gestores de TI precisam se debruçar em soluções de segurança da informação para garantir a integridade dos dados.



Principais Desafios Atuais

Adotar uma abordagem Zero Trust

Zero Trust é uma iniciativa estratégica que ajuda a impedir violações de dados, eliminando o conceito de confiança total na arquitetura de rede de uma organização. Zero Trust não significa tornar um sistema confiável, mas sim eliminar a confiança no sistema.

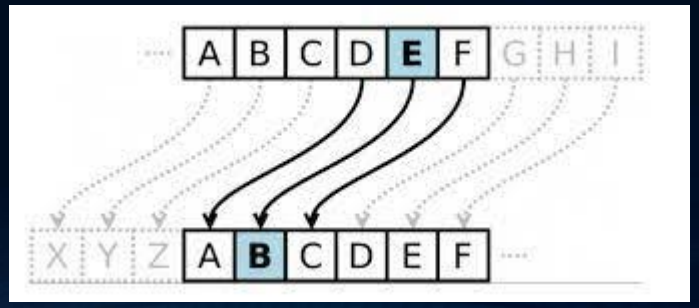
Enraizado no princípio de "nunca confie, sempre verifique, o Zero Trust foi projetado para proteger ambientes digitais modernos, alavancando a segmentação de rede, impedindo movimentos laterais, fornecendo prevenção de ameaças e simplificando o controle granular de acesso do usuário.

Segurança da Informação

Instituto Infnet

Métodos Preventivos

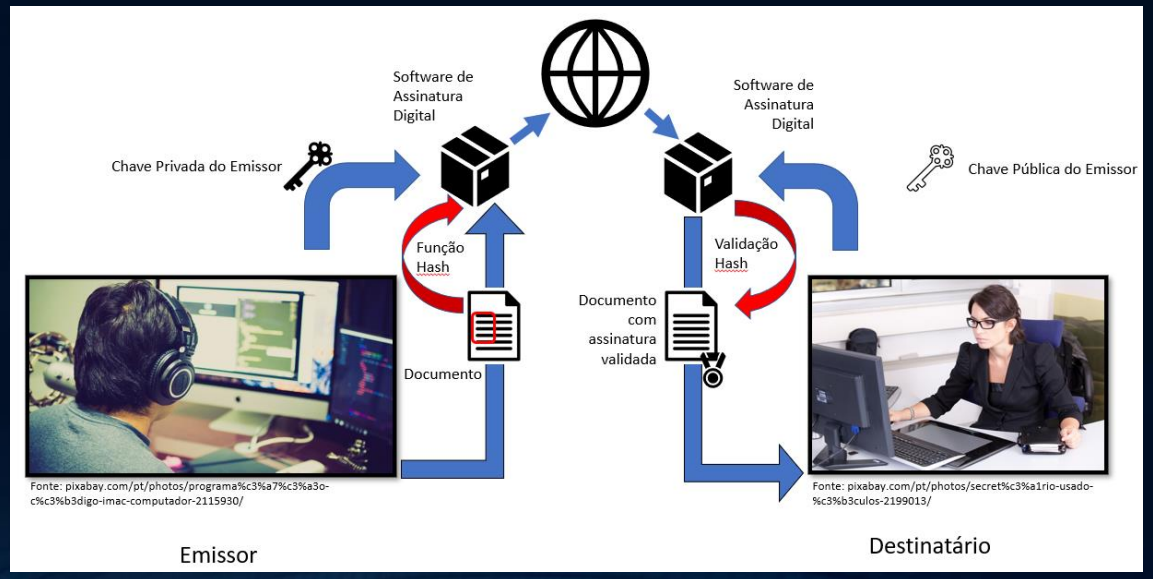
Criptografia: para proteger o conteúdo que trafega pela rede é a encriptação. Se tivéssemos proteção por encriptação, um atacante poderia até conseguir capturar as mensagens, mas não conseguiria ter acesso ao conteúdo. A Criptografia é a ciência de escrever em cifra ou em código. Em outras palavras, ela abarca o conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir normalmente que apenas o destinatário a decifre e a compreenda.



Segurança da Informação

Métodos Preventivos

Assinatura Digital: O processo de geração de uma assinatura digital usa chave criptográfica preferencialmente assimétrica. Para garantir que o documento não foi adulterado, utiliza-se função HASH para validação



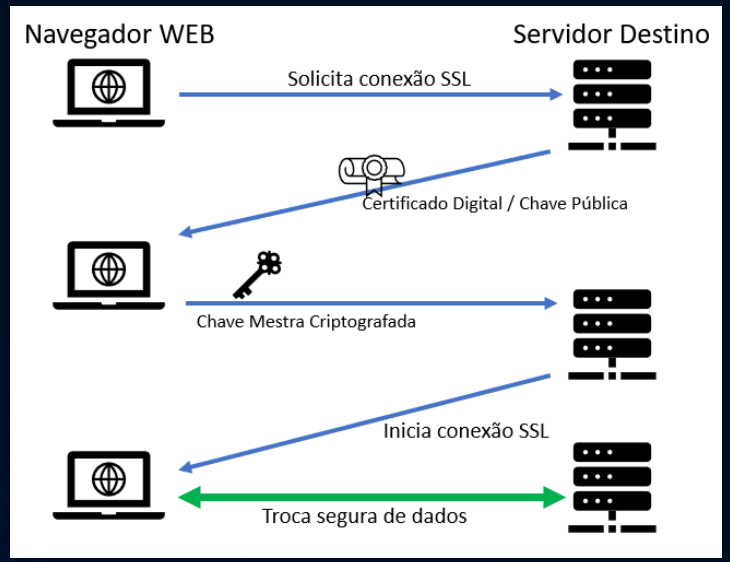
Segurança da Informação

Instituto Infnet

Métodos Preventivos

Protocolo seguro de Transferência: HTTPS (Hyper Text Transfer Protocol Secure)
Esse é um protocolo para transferência de textos e endereços de objetos (como fotos e vídeos). Qualquer informação tramitada por ele será feita como texto simples, inclusive seus dados pessoais

Acrescenta uma camada de segurança na transferência de informações, garantindo que, caso sejam interceptadas, seu conteúdo não poderá ser compreendido.
Inclui um protocolo denominado SSL (Secure Sockets Layer) e nas versões mais recentes o TLS (Transport Layer Security) .



Segurança da Informação

Instituto Infnet

Métodos Preventivos

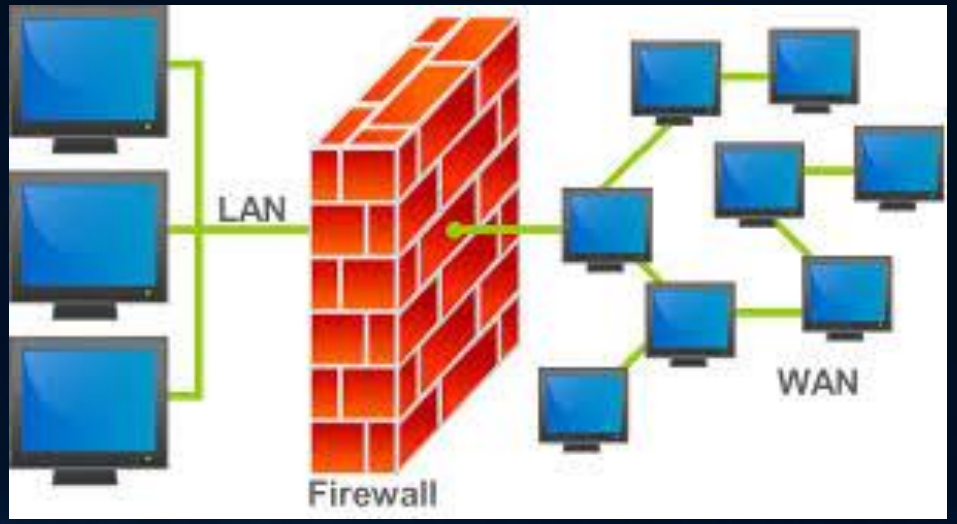
Tecnologias de segurança de perímetro: é fundamental atuar em conjunto com tecnologias de defesa sempre atualizadas, como Firewalls, IPS, Controle de Logs, Antivírus, Área DMZ, etc.

Segurança da Informação

Instituto Infnet

Métodos Preventivos

Firewall: Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança



Segurança da Informação

Instituto Infnet

Métodos Preventivos

Tipos de Firewall:

Firewall de proxy
Um firewall de proxy é um dos primeiros tipos de firewall e funciona como a passagem de uma rede para outra de uma aplicação específica. Servidores proxy podem oferecer recursos adicionais, como armazenamento em cache e segurança de conteúdo ao evitar conexões diretas de fora da rede. No entanto, isso também pode afetar a capacidade de taxa de transferência e as aplicações que eles podem comportar.

Segurança da Informação

Instituto Infnet

Métodos Preventivos

Tipos de Firewall:

Firewall com inspeção de estado
Atualmente conhecido como o firewall tradicional, um firewall com inspeção de estado permite ou bloqueia tráfego de acordo com o estado, a porta e o protocolo. Ele monitora toda atividade desde o momento em que uma conexão é aberta até que ela seja fechada. As decisões de filtragem são tomadas de acordo com as regras definidas pelo administrador e com o contexto, o que significa o uso de informações de conexões e pacotes anteriores que pertencem à mesma conexão

Segurança da Informação

Instituto Infnet

Métodos Preventivos

Tipos de Firewall:

Access Control List (ACL)

Summary | **Inbound Rules** | Outbound Rules | Subnet Associations | Tags

Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Edit

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
1	All ICMP	ICMP (1)	ALL	0.0.0.0/0	ALLOW
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
200	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
300	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
1000	Custom TCP Rule	TCP (6)	1024-65535	10.0.0.0/16	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Segurança da Informação

Instituto Infnet

Métodos Preventivos

Tipos de Firewall:

Firewall de próxima geração (NGFW)
Os firewalls evoluíram para além da simples filtragem de pacotes e inspeção stateful. A maioria das empresas está implantando firewall de próxima geração para bloquear ameaças modernas, como malware avançado e ataques na camada da aplicação.

Recursos padrão de firewall, como inspeção stateful
Prevenção de invasão integrada
Reconhecimento e controle da aplicação para detectar e bloquear aplicativos nocivos
Atualização de caminhos para incluir feeds futuros de informação

Segurança da Informação

Instituto Infnet

Métodos Preventivos

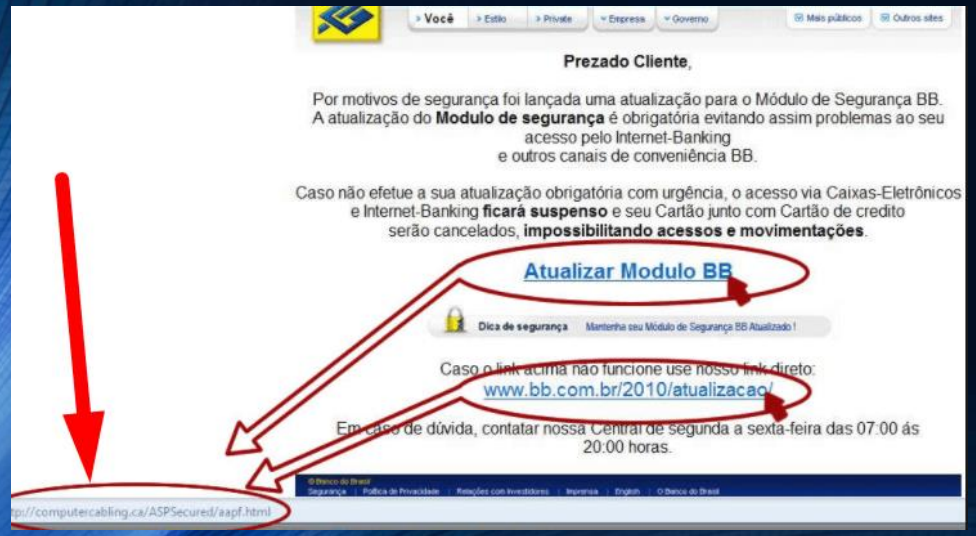
Normas e Políticas de Segurança : Estabelecer regras e normas de conduta em conformidade com leis e normas internacionais, programas de conscientização dos funcionários, entre outros, dará um passo à frente nessa batalha interminável entre a proteção e a invasão dos dados.

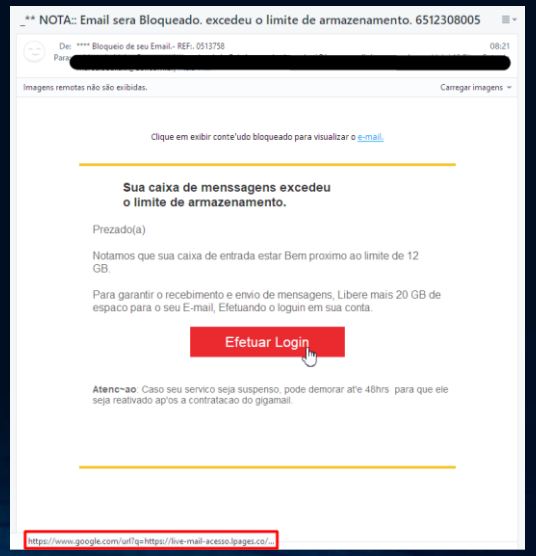
Segurança da Informação

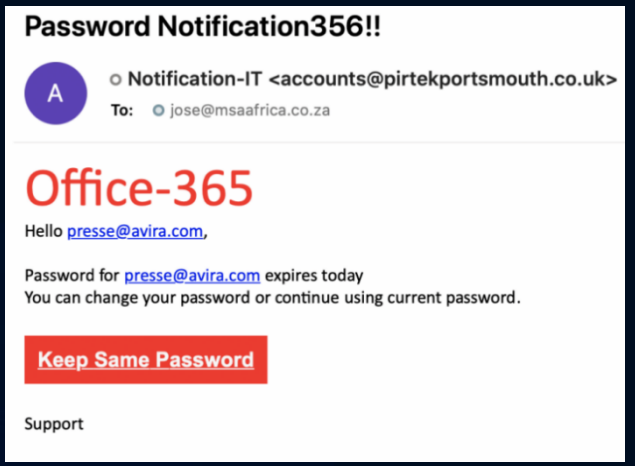
Instituto Infnet

Métodos Preventivos

Comunicação e treinamento em segurança: Capacita TODO o corpo funcional de uma organização à conter ou ao menos minimizar as vulnerabilidades passivas e com isso fechar a porta de entrada para malwares e invasores.





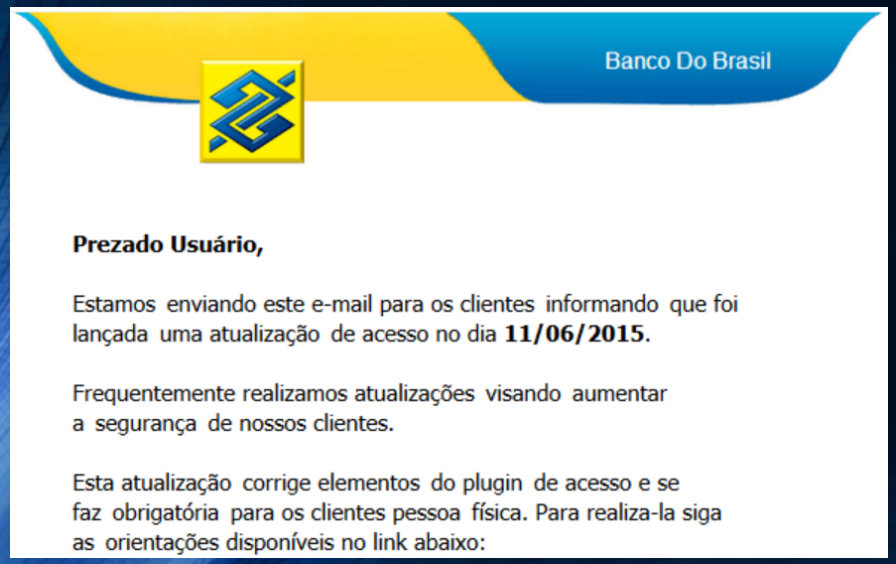


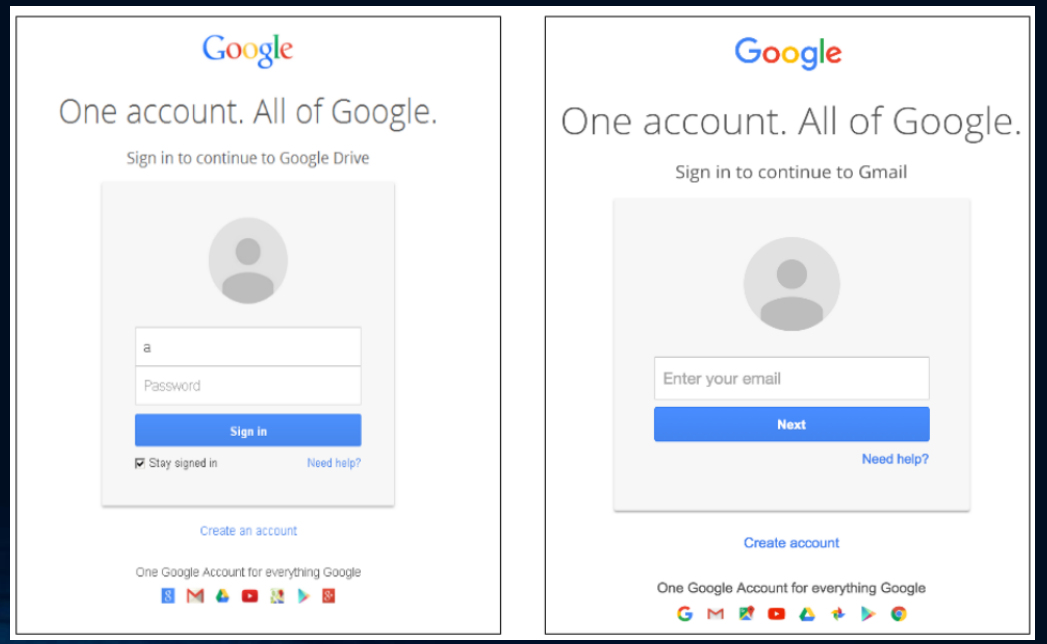
Segurança da Informação

Defendendo de Phishing

Atenção – Calma – Análise – Confirmação na fonte

Sintomas: indução ao medo, ganância, pressa para clicar no link. URL alterada.





Segurança da Informação

Instituto Infnet

Exercícios

Por que você deveria se preocupar com a privacidade de dados? Selecione todas as opções que se aplicam.

A) Ela afeta a todos, no mundo inteiro.

B) A privacidade de dados só se aplica aos empregadores e coletores de dados. Portanto, não é algo com que você deva se preocupar.

C) Muitas vezes, as violações de privacidade têm consequências de longo prazo tanto para indivíduos quanto para organizações.

D) Ao compreender a privacidade de dados, você pode ajudar nossa organização a proteger as informações coletadas.

Segurança da Informação

Instituto Infnet

Exercícios

Qual das seguintes afirmações é a mais precisa no que diz respeito à privacidade e à segurança?

A) Elas são palavras diferentes que descrevem a mesma coisa.

B) Privacidade significa usar os dados somente para os fins a que se destinam e que foram acordados.

C) Segurança é a maneira pela qual a privacidade é mantida.

D) A tecnologia moderna tornou possível alcançar 100% de privacidade e segurança.

E) A privacidade e a segurança só podem ser alcançadas pelo uso de processos altamente técnicos.

Segurança da Informação

Instituto Infnet

Exercícios

As violações de dados, que consistem no vazamento intencional ou não intencional de informações confidenciais, representam uma grande ameaça às organizações do mundo todo. Qual é a causa número um dessas violações?

Erros Humanos

Falhas de sistemas

Ataques cyber criminosos

Antimalware desatualizado

FIM DA ETAPA 02