PGE
Mato Grosso do Sul

Procuradoria-Geral
do Estado

GUIA

de Prevenção a Incidentes de Segurança Cibernético

UPD - PGE/MS - Unidade de Proteção de Dados Pessoais 1ª Edição | 2025

PGE
Mato Grosso do Sul
Procuradoria-Geral do Estado

Administração Superior

Ana Carolina Ali Garcia
Procuradora-Geral do Estado

Márcio André Batista de Arruda
Procurador-Geral Adjunto do Estado do Contencioso

Ivanildo Silva da Costa
Procurador-Geral Adjunto do Estado do Consultivo

Elaboração – conteúdo

Cristiane Müller Dantas
Procuradora do Estado e Encarregada pelo Tratamento de Dados Pessoais

Revisão

Elcia Tatiane Pazeto Puks Campos

Diagramação

Elcia Tatiane Pazeto Puks Campos

Capa

Guido Brey Jr.

2025

PGE
Mato Grosso do Sul
Procuradoria-Geral do Estado

Procuradoria-Geral do Estado de Mato Grosso do Sul (PGE/MS)

Unidade de Proteção de Dados Pessoais (UPD)

Guia de Prevenção a Incidentes de Segurança Cibernéticos. Procuradoria-Geral do Estado de Mato Grosso do Sul. Campo Grande-MS: PGE/MS, 2025.

1. Procuradoria-Geral do Estado. 2. Mato Grosso do Sul. 3. LGPD. 4. Guia de prevenção. 5. Incidentes de Segurança Cibernéticos.

Sumário

Apresentação

A Lei Geral de Proteção de Dados (LGPD) prevê diretrizes taxativas para o tratamento de dados pessoais nos meios físicos e digitais.

Em recepção à LGPD, a Unidade de Proteção de Dados Pessoais (UPD) apresenta o Guia de Prevenção a Incidentes de Segurança Cibernéticos como iniciativa proativa em resposta às exigências da LGPD para fomentar a conscientização sobre os perigos digitais.

O material descreve os potenciais riscos à segurança dos dados pessoais e oferece orientação a Procuradores do Estado, servidores e colaboradores em exercício na Procuradoria-Geral do Estado (PGE/MS) acerca das ameaças cibernéticas que nos cercam.

A partir do contexto fático de tratamento de dados físico e digital, o Guia disponibiliza conteúdo que contempla ameaças e medidas preventivas, enfatizando a importância da instrução para mitigar riscos cibernéticos.

Ações preventivas, na abrangência do tratamento de dados, demonstram o compromisso institucional da Procuradoria com a segurança cibernética e a conformidade regulatória.

Cristiane Müller Dantas
Procuradora do Estado
Encarregada pelo Tratamento de Dados Pessoais da PGE/MS

Incidentes de Segurança Cibernéticos podem ser:

1 Acesso Físico ou Lógico Prejudicado ou Impossibilitado

A frase "acesso físico ou lógico prejudicado ou impossibilitado" se refere à situação em que a capacidade de acessar um sistema, rede ou informação é comprometida ou totalmente bloqueada. Essa situação pode ocorrer por diversos motivos e ter consequências significativas, tanto para indivíduos quanto para organizações.

a) Acesso Físico Prejudicado ou Impossibilitado

O que significa?

Refere-se a situações em que o acesso físico a dispositivo, equipamento ou local é impedido ou dificultado.

Exemplos

Roubo de dispositivos (como *laptops, smartphones ou pendrives*).

Danos físicos em equipamentos (por exemplo, um incêndio que destrói servidores).

Restrição de acesso a locais físicos (como um *data center*).

Consequências

Perda de dados.

Interrupção de serviços.

Danos à infraestrutura.

Custos elevados para reparos e substituições.

b) Acesso Lógico Prejudicado ou Impossibilitado

O que significa?

Refere-se a situações em que o acesso a sistemas, redes ou informações é bloqueado por meios digitais[1].

Exemplos

Ataques cibernéticos: *hackers* podem invadir sistemas e bloquear o acesso a dados.

Falhas de *software*: *bugs* ou falhas em *softwares* podem causar instabilidades e impedir o acesso.

Erros de configuração: configurações incorretas podem bloquear o acesso a determinados recursos.

Consequências

Perda de dados.

Disrupção de negócios.

Danos à reputação.

Custos elevados para recuperação de dados e sistemas.

Causas comuns

Ataques cibernéticos: *hackers* exploram vulnerabilidades em sistemas para obter acesso não autorizado.

Erros humanos: configurações incorretas, perda de senhas ou cliques em *links* maliciosos podem causar problemas de acesso.

Desastres naturais: incêndios, inundações e outros eventos naturais podem danificar equipamentos e interromper serviços.

Falhas de *hardware*: dispositivos como discos rígidos podem falhar e causar perda de dados.

Medidas preventivas

Segurança física: controles de acesso, sistemas de vigilância e *backups* regulares.

Segurança da informação: senhas fortes, autenticação de dois fatores, *firewalls* e *softwares* de segurança.

Planos de recuperação de desastres: procedimentos para restaurar sistemas e dados em caso de incidentes.

Treinamento de funcionários: conscientização sobre as melhores práticas de segurança da informação.

1 Item 6.5 do Política de Segurança da Informação (PSI).

2 Acesso não autorizado

Ocorre quando uma pessoa ou programa ganha acesso a um sistema, rede ou dados sem ter a permissão para isso. É como se alguém entrasse na sua casa sem bater à porta e começasse a mexer em suas coisas.

Por que é um problema?

- **Violação de privacidade:** seus dados pessoais, como senhas, informações financeiras e registros médicos, podem ser expostos.
- **Danos financeiros**: *hackers* podem roubar dinheiro ou causar prejuízos financeiros.
- **Disrupção de serviços:** sistemas podem ser danificados ou sobrecarregados, causando interrupções nos serviços.
- **Reputação:** a violação de segurança pode danificar a reputação de uma organização ou indivíduo.

Como acontece?

Existem diversas formas de acesso não autorizado, incluindo:

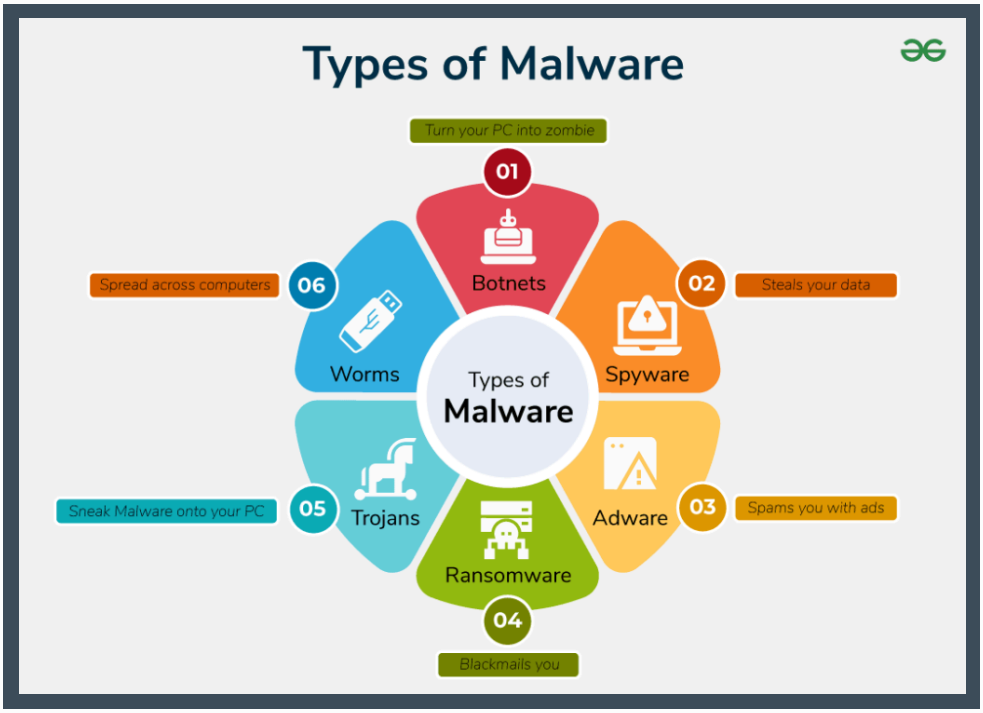
- ***Hacking***: ataques cibernéticos para explorar vulnerabilidades em sistemas.
- ***Phishing:*** enganação para obter informações confidenciais, como senhas.
- ***Malware***: *softwares* maliciosos que infectam dispositivos e roubam dados.
- **Erros humanos:** configurações incorretas ou falha em seguir procedimentos de segurança.

Como se proteger?[2]

- **Senhas fortes:** crie senhas complexas e únicas para cada conta.
- ***Software* atualizado:** mantenha seus sistemas e aplicativos sempre atualizados.
- **Cuidado com *e-mails* e *links* suspeitos:** não clique em *links* ou abra arquivos de remetentes desconhecidos.
- ***Firewall* e antivírus:** utilize ferramentas de segurança para proteger seus dispositivos.
- **Educação:** esteja sempre atento às últimas ameaças cibernéticas e aprenda a se proteger.

2 Conforme item 5 da Política de Controle de Acesso da Política de Segurança da Informação (PSI).

3 **Ataques cibernéticos:** ações em meio digital como *malware*[3], *ransomware*[4], *phishing*[5] e Engenharia Social.[6]



Tradução do quadro pelo Gemini em 26 dez. 2024.

- **Tipos de *Malwares***
- ***Malwares*: conheça os Tipos**
- **Ameaças digitais: tipos de *Malwares***

Tradução das Legendas

Botnets: redes de *bots* (robôs).
Spyware: espião de *software*.
Adware: anúncios indesejados.
Ransomware: sequestro de dados.
Worms: vermes (programas que se autopropaga).
Trojans: Cavalo de Tróia (programa disfarçado).

Descrição dos Quadrantes

- Quadrante 1 (*Botnets*): transforma seu PC em um zumbi.
- Quadrante 2 (*Spyware*): rouba seus dados.
- Quadrante 3 (*Adware*): enche seu dispositivo de anúncios.
- Quadrante 4 (*Ransomware*): sequestra seus arquivos e exige resgate.
- Quadrante 5 (*Trojans*): infiltra *malware* em seu PC de forma disfarçada.
- Quadrante 6 (*Worms*): espalha-se rapidamente por sua rede.

3 É um termo genérico para qualquer tipo de *software* malicioso que pode prejudicar um dispositivo, serviço ou rede, isso inclui vírus e cavalos de Tróia. O objetivo do *malware* é explorar ou danificar o dispositivo, roubando informações ou fazendo com que ele funcione mais lentamente. O *malware* pode ser encontrado em anexos de *e-mail*, mensagens de texto, programas de compartilhamento de arquivos, sites de redes sociais, compartilhamentos de rede e unidades removíveis. Alguns sinais de que um dispositivo pode estar infectado por malware são: Declínio de desempenho, Atividade de rede inesperada, Configurações alteradas, Alertas de eventos de segurança.

4 É um tipo de *malware* que impede o acesso a dados de uma vítima, ameaçando mantê-los bloqueados até que um resgate seja pago ao invasor.
Como funciona: criptografa arquivos e adiciona extensões aos dados, mantendo-os como reféns até que o resgate seja pago.
Como se espalha: por meio de anexos de *e-mail* maliciosos, *download* de arquivos infectados, sites comprometidos e exploração de vulnerabilidades em *softwares* desatualizados.
Tipos: Armários de tela, criptografando, MBR, híbrido.
O *ransomware* pode ser usado para prejudicar grandes empresas, governos federais, infraestrutura global e organizações de saúde. Existem outros tipos de chantagens virtuais, como: mensagens falsas sobre aplicativos e programas não licenciados; falsas alegações sobre conteúdo ilegal; *Doxware* (ou *leakware*), que ameaça publicar informações roubadas online. Disponível em: https://www.ibm.com/br-pt/topics/ransomware#:~:text=O%20ransomware%20%C3%A9%20um%20tipo,pague% 20um%20resgate %20ao%20invasor, https://www.kaspersky.com.br/resource-center/threats/ransomware, https://www.akamai.com/pt/glossary/what-is-ransomware#:~:text=Entendendo%20o%20ransomware,global%20e%20organiza%C3%A7%C3%B5es%20de%20sa%C3%BAde. Acesso em: 30 set. 2024.

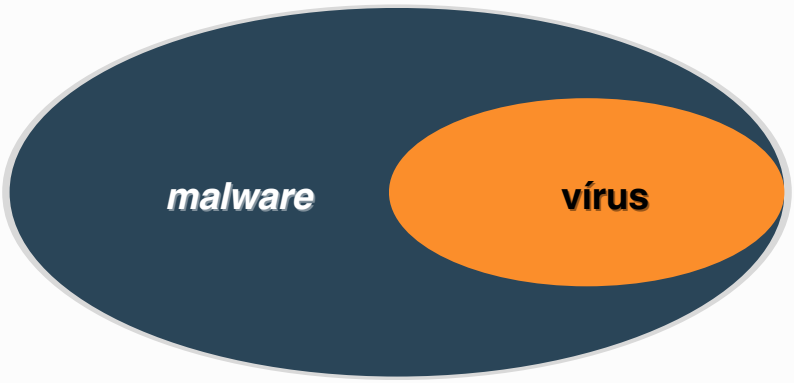
5 Disponível em: https://www.geeksforgeeks.org/malware-and-its-types/. Acesso em: 26 dez. 2024.

6 A Engenharia Social é uma técnica de manipulação que explora erros humanos para obter informações privadas, acessos ou coisas de valor.

Malwares

Vírus

Embora muitas pessoas confundam *malwares* com vírus, eles não são a mesma coisa. A explicação é a seguinte: todo *vírus* é um malware, mas nem todo *malware* é um *vírus*.



O *malware* se espalha fazendo cópias de si mesmo em outros *softwares*.
Geralmente, o dispositivo é infectado quando você baixa algum arquivo ou programa contaminado, por meio de ataques *phishing*. O pior é que você pode acabar transmitindo para outras pessoas ao encaminhar um *e-mail* ou emprestar um *pendrive*, por exemplo.

Os *vírus* são *softwares* maliciosos que infectam programas e arquivos. A propagação ocorre da mesma maneira que o vírus conhecido na biologia.

Worms

Os *worms* são um tipo de *malware* semelhante ao vírus, já que eles também se propagam pelo seu dispositivo de forma automática e contaminam programas e arquivos.

A grande diferença é que eles não precisam da sua ação para se disseminarem para outros dispositivos. Os *worms* acessam a lista de contatos do hospedeiro e se espalham por *e-mails*, SMS e aplicativos de mensagens.

Cavalos de Tróia

Os Cavalos de Tróia, também conhecido como *trojans*, são *malwares* que se disfarçam de *softwares* legítimos para executarem alguma tarefa maliciosa no seu dispositivo.

Ao contrário do vírus e do *worm*, o trojan não tem capacidade de se multiplicar sozinho. Ainda assim, apresenta um grande risco, já que abre brechas para ataques cibernéticos e roubo de dados.

Adwares

Os *adwares* são aplicativos maliciosos que objetivam encher o seu dispositivo de publicidade indesejada. Eles afetam principalmente o navegador do seu computador, celular ou *tablet*.

Além de apresentarem anúncios mal-intencionados, os *adwares* podem piorar o funcionamento do seu dispositivo, afetar o gasto da bateria e aumentar o consumo de internet.

Spywares

Os *spywares* são programas espiões que coletam informações no seu dispositivo e enviam para os criadores do *malware*, sem o seu consentimento.

A espionagem pode ser desde dados simples, como o seu padrão de comportamento na internet, até super sensíveis, como senhas e informações bancárias.

Botnets

Já os *bots* e *botnets* transformam o seu dispositivo em zumbi e geralmente permitem que um terceiro realize tarefas de forma remota, sem que você perceba, já que eles se camuflam no sistema.

Na maioria das vezes, os *bots* operam em grande escala, afetando vários dispositivos ao mesmo tempo[7].

Ransomware

O *ransomware* captura um sistema de computador ou os dados que nele contém até que a vítima faça um pagamento[8].

7 Disponível em: https://blog.picpay.com/virus-no-celular/. Acesso em: 26 dez. 2024.
8 Disponível em: https://www.geeksforgeeks.org/malware-and-its-types/. Acesso em: 26 dez. 2024.

Phishing

Phishing é um tipo de ataque cibernético que usa *e-mails,* mensagens de texto, chamadas telefônicas ou sites fraudulentos para induzir as pessoas a compartilharem dados confidenciais, baixarem ***malware*** ou se exporem ao crime cibernético.

Ataques de *phishing* são uma forma de E**ngenharia Social**. Diferentemente de outros ataques **cibernéticos** que visam diretamente redes e recursos, os ataques de engenharia social usam erro humano, **histórias falsas** e táticas de pressão para manipular as vítimas para que elas mesmas ou suas organizações sejam prejudicadas involuntariamente.

Em um golpe de *phishing* típico, um ***hacker*** finge ser alguém em quem a vítima confia, como um colega, chefe, figura de autoridade ou representante de uma marca bem conhecida. O *hacker* envia uma mensagem direcionando a vítima a pagar uma fatura, a abrir um anexo, a clicar em um *link* ou a tomar alguma outra ação.

Como confia na suposta fonte da mensagem, o usuário segue as instruções e cai direto na armadilha do golpista. Essa "fatura" pode levar diretamente à conta de um *hacker*. Esse anexo pode instalar ***ransomware*** no dispositivo do usuário. Esse *link* pode levar o usuário a um site que rouba números de cartão de crédito, números de conta bancária, credenciais de *login* ou outros **dados pessoais.**

Por que o *phishing* é uma grande ameaça cibernética?

Phishing é popular entre criminosos cibernéticos e altamente eficaz. De acordo com o relatório *Cost of a Data Breach da IBM, phishing* é o vetor de violação de dados mais comum, respondendo por 15% de todas as violações. Violações causadas por *phishing* custam às organizações uma média de ***USD 4,88 milhões***.

Phishing é uma ameaça significativa porque explora pessoas em vez de vulnerabilidades tecnológicas. Os invasores não precisam violar sistemas diretamente ou enganar ferramentas **de segurança cibernética**. Eles podem enganar pessoas que têm acesso autorizado ao seu alvo — seja dinheiro, informações confidenciais ou outra coisa — para fazerem seu trabalho sujo.

***Phishers* podem ser golpistas solitários ou gangues criminosas sofisticadas. Eles podem usar *phishing* para muitos fins maliciosos, incluindo roubo de identidade, fraude de cartão de crédito, roubo monetário, extorsão, apropriação indébita de contas, espionagem e muito mais.**

Os alvos de *phishing* variam de pessoas comuns a grandes corporações e agências governamentais. Em um dos ataques de *phishing* mais conhecido, *hackers* russos usaram um *e-mail* falso de redefinição de senha para roubar milhares de *e-mails* da campanha presidencial de Hillary Clinton em 2016 nos EUA.

Como os golpes de *phishing* manipulam seres humanos, as ferramentas e as técnicas de monitoramento de rede padrão nem sempre conseguem capturar esses ataques em andamento. De fato, no ataque da campanha de Clinton, até mesmo o *help desk* de TI da campanha pensou que os *e-mails* fraudulentos de redefinição de senha eram autênticos.

Para combater o *phishing*, as organizações devem combinar ferramentas avançadas de detecção de ameaças com uma sólida educação dos funcionários para garantir que os usuários possam identificar com precisão e responder com segurança às tentativas de golpe.

Tipos de ataques de *phishing*

A palavra "***phishing***" brinca com o fato de que os golpistas usam "iscas" atraentes para enganar suas vítimas, da mesma forma que os pescadores usam iscas para fisgar peixes de verdade. No *phishing*, as iscas são mensagens fraudulentas que parecem confiáveis e evocam emoções fortes como medo, ganância e curiosidade.

Os tipos de iscas que os golpistas de *phishing* usam dependem de quem e do que eles estão atrás. Alguns exemplos comuns de ataques de *phishing* incluem:

Phishing de *e-mail* em massa

No *phishing* de *e-mail* em massa, os golpistas enviam indiscriminadamente *e-mails* de *spam* para o maior número possível de pessoas, esperando que uma fração dos alvos caia no ataque.

Os golpistas geralmente criam *e-mails* que parecem vir de empresas grandes e legítimas, como bancos, varejistas *online* ou criadores de aplicativos populares. Ao se passarem por marcas bem conhecidas, os golpistas aumentam as chances de que seus alvos sejam clientes dessas marcas. Se um alvo interage regularmente com uma marca, é mais provável que ele abra um *e-mail* de *phishing* supostamente dessa marca.

Os criminosos cibernéticos fazem de tudo para os *e-mails* de *phishing* parecerem verdadeiros. Eles podem usar o logotipo e a marca do remetente personificado. Eles podem falsificar endereços de *e-mail* para fazer parecer que a mensagem vem do nome de domínio do remetente personificado. Eles podem, até mesmo, copiar um *e-mail* verdadeiro do remetente personificado e modificá-lo para fins maliciosos.

Golpistas escrevem linhas de assunto de *e-mail* para apelar a emoções fortes ou criar um senso de urgência. Golpistas experientes usam assuntos que o remetente personificado pode realmente abordar, como "Problema com seu pedido" ou "Sua fatura está anexada".

O corpo do *e-mail* instrui o destinatário a tomar uma ação aparentemente razoável que resulta na divulgação de informações confidenciais ou no download de *malware*. Por exemplo, um *link* de *phishing* pode dizer: "Clique aqui para atualizar seu perfil". Quando a vítima clica no *link* malicioso, ele a leva para um *site* falso que rouba suas credenciais de *login*.

Alguns golpistas programam suas campanhas de *phishing* para coincidir com feriados e outros eventos em que as pessoas são mais suscetíveis à pressão.

Por exemplo, ataques de *phishing* a clientes da Amazon geralmente aumentam em torno do *Prime Day*, evento anual de vendas do varejista *online*. Os golpistas enviam *e-mails* sobre negócios falsos e problemas de pagamento para tirar vantagem da baixa guarda das pessoas.

Phishing de lança

Spear phishing é um ataque de *phishing* direcionado a um indivíduo específico. O alvo geralmente é alguém com acesso privilegiado a dados sensíveis ou autoridade especial que o golpista pode explorar, como um gerente financeiro que pode movimentar dinheiro de contas da empresa.

Um *spear phisher* estuda seu alvo para reunir as informações de que precisa para se passar por alguém em quem o alvo confia, como um amigo, chefe, colega de trabalho, fornecedor ou instituição financeira. Mídias sociais e sites de redes profissionais — onde as pessoas parabenizam publicamente colegas de trabalho, endossam fornecedores e tendem a compartilhar demais — são fontes ricas de informações para pesquisa de s*pear phishing*.

Spear phishers usam suas pesquisas para elaborar mensagens que contenham detalhes pessoais específicos, fazendo com que pareçam altamente confiáveis para o alvo.

Por exemplo, um *spear phisher* pode se passar pelo chefe do alvo e enviar um *e-mail* que diz: "Sei que você está saindo hoje à noite para férias, mas pode pagar esta fatura antes do fechamento do expediente hoje?"

Um ataque de *spear phishing* direcionado a um executivo de alto escalão, indivíduo rico ou outro alvo de alto valor é chamado de ***whale phishing*** ou ataque *whaling*.

Comprometimento de *e-mail* comercial (BEC)

BEC é uma classe de ataques de *spear phishing* que tentam roubar dinheiro ou informações valiosas — por exemplo, segredos comerciais, dados de clientes ou informações financeiras — de uma empresa ou outra organização.
Ataques BEC podem assumir várias formas. Duas das mais comuns incluem:

Fraude de CEO

O golpista se passa por um executivo de nível C, geralmente sequestrando a conta de *e-mail* do executivo. O golpista envia uma mensagem a um funcionário de nível inferior instruindo-o a transferir fundos para uma conta fraudulenta, fazer uma compra de um fornecedor fraudulento ou enviar arquivos para uma parte não autorizada.

Comprometimento de conta de e-mail (EAC)

O golpista compromete a conta de *e-mail* de um funcionário de nível inferior, como a conta de um gerente em finanças, vendas ou pesquisa e desenvolvimento. O golpista usa a conta para enviar faturas fraudulentas a fornecedores, instruir outros funcionários a fazerem pagamentos fraudulentos ou solicitarem acesso a dados confidenciais.

Os ataques BEC podem estar entre os ataques cibernéticos mais caros, com golpistas frequentemente roubando milhões de dólares de uma vez. Em um exemplo notável, um grupo de golpistas roubou mais de US$ 100 milhões do *Facebook* e do *Google* se passando por um fornecedor legítimo de *software*.

Alguns golpistas de BEC estão se afastando dessas táticas de alto perfil em favor de lançar pequenos ataques contra mais alvos. De acordo com o A*nti-Phishing Working Group (APWG)*, os ataques de BEC se tornaram mais frequentes em 2023, mas os golpistas pediram menos dinheiro em média com cada ataque.

Outras técnicas de *phishing*

Sorrindo

O *phishing* por SMS, ou *smishing*, usa mensagens de texto falsas para enganar os alvos. Os golpistas geralmente se passam pelo provedor de serviços sem fio da vítima, enviando um texto que oferece um "brinde" ou pede que o usuário atualize suas informações de cartão de crédito.

Alguns *smishers* se passam pelo Serviço Postal dos EUA ou outra empresa de transporte. Eles enviam textos dizendo às vítimas que elas devem pagar uma taxa para receber um pacote pedido.

Visitando

Phishing de voz, ou *vishing,* é *phishing* por chamada telefônica. Os incidentes de *vishing* explodiram nos últimos anos, aumentando em 260% entre 2022 e 2023, de acordo com o APWG (Anti-Phishing Working Group). O aumento do *vishing* se deve em parte à disponibilidade da tecnologia de voz sobre IP (VoIP), que os golpistas podem usar para fazer milhões de chamadas de *vishing* automatizadas por dia.

Golpistas geralmente usam falsificação de identificação de chamadas para fazer com que suas chamadas pareçam vir de organizações legítimas ou números de telefone locais. Chamadas de *vishing* geralmente assustam os destinatários com avisos de problemas de processamento de cartão de crédito, pagamentos atrasados ou problemas com a lei. Os destinatários acabam fornecendo dados confidenciais ou dinheiro aos cibercriminosos para "resolverem" seus problemas.

Phishing em mídias sociais

O *phishing* de mídia social emprega plataformas de mídia social para enganar as pessoas. Os golpistas usam os recursos de mensagens integrados das plataformas — por exemplo *Facebook, Messenger, LinkedIn, InMail* e X (antigo *Twitter*) *DMs* — da mesma forma que usam *e-mail* e mensagens de texto.

Golpistas geralmente se passam por usuários que precisam da ajuda do alvo para fazer *login* em sua conta ou ganhar um concurso. Eles usam esse plano para roubar as credenciais de *login* do alvo e assumir o controle de sua conta na plataforma. Esses ataques podem ser especialmente custosos para vítimas que usam as mesmas senhas em várias contas, uma prática muito comum.

Tendências recentes em phishing

Golpistas constantemente criam novas técnicas de *phishing* para evitar a detecção. Alguns desenvolvimentos recentes incluem:

Phishing de IA

O *phishing* de IA usa ferramentas de Inteligência Artificial (IA) generativas para criar mensagens de *phishing*. Essas ferramentas podem gerar *e-mails* e mensagens de texto personalizados que não têm erros de ortografia, inconsistências gramaticais e outros sinais de alerta comuns de tentativas de *phishing*.

A IA generativa também pode ajudar os golpistas a escalarem suas operações. De acordo com o *X-Force Threat Intelligence Index da IBM*, um golpista leva 16 horas para elaborar um *e-mail* de *phishing* manualmente. Com a IA, os golpistas podem criar mensagens ainda mais convincentes em apenas cinco minutos.

Os golpistas também usam geradores de imagens e sintetizadores de voz para adicionar mais credibilidade aos seus esquemas. Por exemplo, em 2019, os invasores usaram IA para clonar a voz do CEO de uma empresa de energia e enganar um gerente de banco em US$ 243.000.

Quishing

Quishing usa códigos QR falsos incorporados em *e-mails* e mensagens de texto ou postados no mundo real. *Quishing* permite que *hackers* escondam *sites* e *softwares* maliciosos à vista de todos.

Por exemplo, a Comissão Federal de Comércio dos EUA (FTC) alertou no ano passado sobre um golpe em que criminosos substituem códigos QR em parquímetros públicos por seus próprios códigos que roubam dados de pagamento.

Vishing híbrido

Ataques de *vishing* híbridos combinam *phishing* de voz com outros métodos para driblar filtros de *spam* e ganhar a confiança das vítimas.

Por exemplo, um golpista pode enviar um *e-mail* alegando vir do IRS. Este *e-mail* informa ao alvo que há um problema com sua declaração de imposto de renda. Para resolver o problema, o alvo deve ligar para um número de telefone fornecido no *e-mail*, que o conecta diretamente ao golpista.

Quais são os sinais de um ataque de *phishing*?

Os detalhes podem variar de golpe para golpe, mas há alguns sinais comuns que indicam que uma mensagem pode ser uma tentativa de *phishing*, como:

Emoções fortes e táticas de pressão

Golpes de *phishing* tentam fazer com que as vítimas sintam uma sensação de urgência para que elas ajam rapidamente sem pensar. Golpistas geralmente fazem isso invocando emoções fortes como medo, ganância e curiosidade. Eles podem impor limites de tempo e ameaçar consequências irrealistas, como prisão.

Truques comuns de *phishing*

- "Há um problema com sua conta ou informações financeiras. Você deve atualizá-las imediatamente para evitar perder o acesso."
- "Detectamos atividade ilegal. Pague esta multa agora, ou então você será preso."
- "Você ganhou um presente grátis, mas precisa reivindicá-lo agora mesmo."
- "Esta fatura está vencida. Você deve pagá-la imediatamente, ou cortaremos seu serviço."
- "Temos uma oportunidade de investimento empolgante para você. Deposite dinheiro agora, e podemos garantir retornos incríveis."

Solicitações de dinheiro ou informações confidenciais

Golpes de *phishing* geralmente pedem uma de duas coisas: **dinheiro ou dados**. Solicitações não solicitadas ou inesperadas de pagamento ou de informações pessoais podem ser sinais de ataques de *phishing*.
Golpistas disfarçam suas solicitações de dinheiro como faturas vencidas, multas ou taxas por serviços. Eles disfarçam solicitações de informações como avisos para atualizar informações de pagamento ou conta ou redefinir uma senha.

Má ortografia e gramática

Muitas gangues de *phishing* operam internacionalmente, o que significa que elas frequentemente escrevem mensagens de *phishing* em idiomas que não falam fluentemente.

Portanto, muitas tentativas de *phishing* contêm erros gramaticais e inconsistências.

A IA está mudando isso, facilitando a elaboração de mensagens sem erros gramaticais e ortográficos.

Mensagens genéricas

Mensagens de marcas legítimas geralmente contêm detalhes específicos.

Elas podem se dirigir aos clientes pelo nome, fazer referência a números de pedidos específicos ou explicar precisamente qual é o problema.

Uma **mensagem vaga** como "Há um problema com sua conta" sem mais detalhes **é um sinal de alerta**.

URLs e endereços de *e-mail* falsos

Golpistas geralmente usam URLs e endereços de *e-mail* que parecem legítimos à primeira vista.

Por exemplo, um *e-mail* de "**admin@rnicrosoft.com**" pode parecer seguro, mas olhe novamente. O "m" **em "*Microsoft*" é, na verdade, um "r" e um "n".**

Outra tática comum é usar uma URL como "***bankingapp.scamsite.com***".

Um usuário pode pensar que isso leva ao *bankingapp.com*, mas na verdade aponta para um subdomínio de scamsite.com.

Hackers também podem usar serviços de encurtamento de *links* para disfarçar URLs maliciosos.

Outros sinais

Golpistas podem enviar arquivos e anexos que o alvo não solicitou e não espera. Eles podem usar imagens de texto em vez de texto real em mensagens e páginas da *web* para evitar filtros de *spam*.

Alguns golpistas fazem referência a questões polêmicas para irritar as vítimas. Por exemplo, a I*BM® X-Force®* descobriu que os golpistas geralmente usam o conflito na Ucrânia para atiçar as emoções dos alvos.

Prevenção e mitigação de *phishing*

Treinamento de conscientização sobre segurança e políticas organizacionais

Como os golpes de *phishing* têm como alvo pessoas, **os funcionários geralmente são a primeira e a última linha de defesa de uma organização contra esses ataques.**

As organizações podem ensinar os usuários a reconhecerem os sinais de tentativas de *phishing* e responderem *e-mails* e mensagens de texto suspeitos.

Isso pode incluir dar aos funcionários maneiras fáceis de relatarem tentativas de *phishing* à equipe de TI ou segurança.

As organizações também podem estabelecer políticas e práticas que dificultem o sucesso dos *phishers*

Por exemplo, as organizações podem proibir as pessoas de iniciar transferências monetárias por *e-mail*.

Elas podem exigir que os funcionários verifiquem solicitações de dinheiro ou informações entrando em contato com o solicitante por meios diferentes dos fornecidos na mensagem.

Por exemplo, os funcionários podem digitar uma URL diretamente no navegador em vez de clicar em um *link* ou ligar para o telefone do escritório de um colega em vez de responder a uma mensagem de texto de um número desconhecido.

Ferramentas e tecnologia *antiphishing*

As organizações podem complementar o treinamento de funcionários e as políticas da empresa com ferramentas de segurança que ajudam detectar mensagens de *phishing* e frustrar *hackers* que usam *phishing* para invadir redes.

Filtros de spam e *software* de segurança de *e-mail*

Usam dados sobre golpes de *phishing* existentes e algoritmos ***de aprendizado de máquina*** para identificar *e-mails* de *phishing* e outras mensagens de *spam*. Os golpes e *spam* são então movidos para uma pasta separada, onde *links* e códigos maliciosos são erradicados.

Softwares* antivírus e *antimalware

Podem detectar e neutralizar arquivos ou códigos maliciosos transportados por *e-mails* de *phishing*.

A autenticação multifator

Pode impedir que *hackers* tomem conta de usuários.

Phishers podem roubar senhas, mas têm muito mais dificuldade em roubar um segundo fator, como uma digitalização de impressão digital ou uma senha de uso único.

Ferramentas de segurança de *endpoint*

Como soluções de *detecção e resposta de* endpoint *(EDR)* e *gerenciamento unificado de endpoint* (UEM), podem usar IA e análises avançadas para interceptar tentativas de *phishing* e bloquear *malware*.

Os filtros da *Web*

Impedem que os usuários visitem *sites* maliciosos conhecidos e exibam alertas sempre que os usuários visitam páginas suspeitas.

Essas ferramentas podem ajudar a mitigar danos se um usuário clicar em um *link* de *phishing*.

Soluções de segurança cibernética corporativa

Como *orquestração de segurança, automação e resposta (SOAR)* e plataformas *de gerenciamento de informações e eventos de segurança (SIEM)*, usam IA e automação para detectar e responder a atividades anômalas. Essas soluções podem ajudar a impedir *phishers* que estão tentando instalar *malware* ou assumir contas[9].

9 Disponível em: https://www.ibm.com/think/topics/phishing. Acesso em: 26 dez. 2024.

Engenharia Social

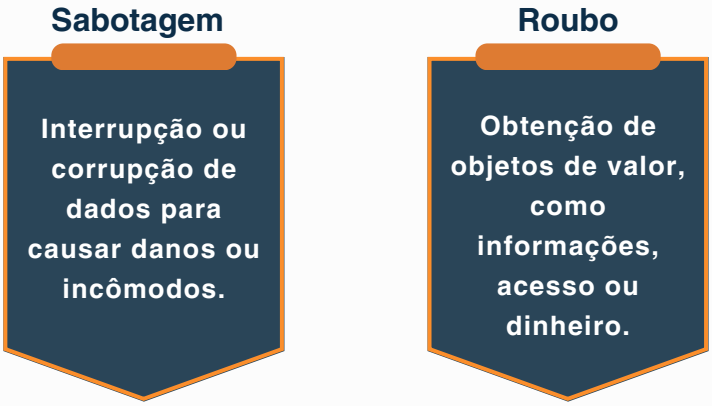
Definição de Engenharia Social

A engenharia social é técnica de manipulação que explora erros humanos para obter informações privadas, acessos ou coisas de valor. No crime cibernético, esses golpes de "*hacking* humano" tendem a atrair usuários desavisados para exporem dados, espalharem infecções por *malware* ou permitirem acesso a sistemas restritos. Os ataques podem acontecer *online*, em pessoa e por outros meios de interação.

Os golpes promovidos com base em Engenharia Social são feitos a partir de como as pessoas pensam e agem. Sendo assim, os ataques de engenharia social são especialmente úteis para manipular o comportamento de um usuário. Quando um invasor entende o que motiva as ações de um usuário, ele pode enganar e manipular o usuário de forma eficaz.

Além disso, os *hackers* tentam explorar a falta de conhecimento do usuário. Graças à velocidade da tecnologia, muitos consumidores e funcionários não reconhecem certas ameaças como os *downloads* automáticos. **Os usuários podem também não perceber o verdadeiro valor dos dados pessoais, como o seu número do telefone, por exemplo. Por isso, muitos usuários não sabem exatamente como proteger a si mesmo e seus dados.**

Em geral, os invasores de Engenharia Social têm um dos seguintes objetivos:



Essa definição de Engenharia Social pode ser expandida ainda mais se soubermos exatamente como ela funciona.

Como funciona a Engenharia Social?

A maioria dos ataques de Engenharia Social depende da comunicação real entre os atacantes e as vítimas. O invasor tende a motivar o usuário a se comprometer, em vez de usar **métodos de força bruta** para violar seus dados.

O ciclo de ataque oferece a esses criminosos um processo confiável para enganar você.

Os passos para o ciclo de ataque de Engenharia Social geralmente são:

Preparar	Infiltrar-se	Explorar a vítima	Desvincular-se
Reunir informações sobre seu histórico ou de um grupo maior do qual você faz parte.	Estabelecer um relacionamento ou iniciando uma interação, que começa pela construção de confiança.	Uma vez que a confiança e uma vulnerabilidade sejam estabelecidas para avançar com o ataque.	Assim que o usuário tiver realizado a ação desejada.

Esse processo pode ocorrer em um único *e-mail* ou ao longo de meses, em uma série de conversas nas redes sociais. Poderia até ser uma interação cara a cara. Mas, no fim das contas, tudo acaba em uma ação que você realiza, como compartilhar suas informações ou se expor a *malwares*.

É importante ter cuidado com a Engenharia Social usada para confundir as pessoas. **Muitos funcionários e consumidores não percebem que apenas algumas peças de informação podem dar acesso a *hackers* e a várias redes e contas.**

Ao se passarem por usuários legítimos para os funcionários de suporte de TI, eles obtêm seus dados privados — como nome, data de nascimento ou endereço. A partir daí, é só uma questão de redefinirem senhas e obterem acesso praticamente ilimitado. Podem roubar dinheiro, espalhar *malware* de Engenharia Social e muito mais.

Características dos ataques de Engenharia Social

Os ataques de engenharia social giram em torno do uso de persuasão e confiança pelo atacante. Quando exposto a essas táticas, é mais provável que você tome atitudes que não tomaria em outras circunstâncias.

Nos ataques, a maioria das vezes, você será induzido aos seguintes comportamentos:

Emoções intensificadas

A manipulação emocional dá aos agressores a vantagem em qualquer interação. Você fica muito mais propenso a praticar ações arriscadas e irracionais sob um estado emocional abalado. As seguintes emoções são todas usadas na mesma proporção para convencê-lo.

- Medo
- Empolgação
- Curiosidade
- Raiva
- Culpa
- Tristeza

Urgência

Oportunidades ou solicitações sensíveis ao tempo são outra ferramenta confiável no arsenal de um invasor. Você pode cair na armadilha sob o pretexto de um problema sério que precisa de atenção imediata. Outra possibilidade é você se expor porque há um prêmio ou uma recompensa que pode desaparecer se você não agir rapidamente. Tanto uma quanto outra abordagem desativa sua capacidade de pensamento crítico.

Confiança

A credibilidade é inestimável e essencial para um ataque de Engenharia Social. Como o atacante está mentindo para você, a confiança desempenha um papel importante aqui. Eles fizeram pesquisas suficientes sobre você para criar uma narrativa fácil de acreditar e improvável de levantar suspeitas.

Há algumas exceções a essas características. Em alguns casos, os invasores usam métodos mais simples de Engenharia Social para conseguir acessar a rede ou o computador. Por exemplo, um *hacker* pode frequentar a praça de alimentação de um edifício corporativo e bisbilhotar os usuários que trabalham com *tablets* ou *laptops*. Assim, pode conseguir um grande número de senhas e nomes de usuários, sem enviar sequer um *e-mail* ou escrever uma linha de código de vírus.

⚠ Agora que você entende o conceito subjacente, provavelmente está se perguntando "o que é um ataque de engenharia social e como posso identificá-lo?"

Tipos de ataques de Engenharia Social

Praticamente todo tipo de ataque à cibersegurança contém algum método de Engenharia Social. Por exemplo, os golpes clássicos de *e-mail* e vírus estão carregados de conotações sociais.

A Engenharia Social pode impactar você digitalmente por meio de ataques a dispositivos móveis, além de dispositivos de mesa. No entanto, você também pode sofrer uma ameaça pessoalmente. Esses ataques podem se sobrepor e se acumular uns aos outros para criar um golpe.

Seguem alguns métodos comuns de Engenharia Social mobilizados pelos golpistas.

Ataques de *phishing*

Os golpistas do *phishing* fingem ser uma instituição ou um indivíduo confiável na tentativa de persuadi-lo a expor dados pessoais e outros bens valiosos. Os ataques que utilizam o *phishing* são direcionados de duas maneiras:

O *spam* de *phishing*

Ou *phishing* em massa, é um ataque generalizado dirigido a muitos usuários.

Esses ataques não são personalizados e tentam pegar qualquer pessoa desprevenida.

Spear phishing*, por extensão, o *whaling

Utilizam informações personalizadas para direcionar usuários específicos. Os ataques de *whaling* visam especificamente alvos de alto valor, como celebridades, altos executivos e autoridades governamentais.

As chamadas telefônicas de ***phishing* de voz (*vishing*)** podem ser sistemas de mensagens automatizadas que gravam todas as suas entradas. Às vezes, uma pessoa ao vivo pode falar com você para aumentar a confiança e a urgência.

Textos de ***phishing* por SMS (*smishing*)** ou mensagens de aplicativos móveis podem incluir um *link* da *web* ou uma solicitação para seguir através de um *e-mail* fraudulento ou número de telefone.

O ***phishing* por e-mail é** o meio mais tradicional de *phishing*, utilizando um *e-mail* urgente solicitando a sua resposta ou acompanhamento por outros meios. *Links* da *web*, números de telefone ou anexos de *malware* podem ser utilizados.

O ***angler phishing*** ocorre nas redes sociais, onde um atacante imita a equipe de atendimento ao cliente de uma empresa confiável. Eles interceptam suas comunicações com uma marca para sequestrar e desviar sua conversa para mensagens privadas para avançarem com o golpe.

***Phishing* de buscador** é uma tentativa de colocar *links* para *sites* falsos no topo dos resultados da busca. Esses podem ser anúncios pagos ou usar métodos legítimos de otimização para manipular os *rankings* de busca.

Links de ***phishing* de URL** tentam você a visitar *sites* de *phishing*. Esses *links* são comumente entregues em *e-mails*, mensagens de texto de redes sociais e anúncios *online*. Os ataques escondem *links* em textos ou botões de hiperlink, utilizando ferramentas de encurtamento de *links* ou URLs com grafias enganosas.

O ***phishing* em sessão** aparece como uma interrupção na sua navegação normal na *web*. Por exemplo, você pode ver *pop-ups* de *logins falsos* para as páginas que você está visitando no momento.

Golpes de *baiting*

O *baiting* abusa de sua curiosidade natural para o convencer a se expor a um agressor. Tipicamente, o potencial de receber algo gratuito ou exclusivo é usado para manipulá-lo e explorá-lo. O golpe normalmente consiste em infectar você com *malware*.

Os métodos populares de *baiting* podem incluir:

- p*endrives* deixados em espaços públicos, como bibliotecas e estacionamentos;
- anexos de *e-mail* incluindo detalhes sobre uma oferta gratuita ou *software* gratuito fraudulento.

Golpes de violação física

As violações físicas envolvem invasores aparecendo pessoalmente, passando-se por alguém legítimo para obter acesso a áreas ou a informações não autorizadas.

Os golpes desse tipo são mais comuns em ambientes empresariais, como governos, empresas ou outras organizações. Os golpistas podem fingir ser um representante de um fornecedor conhecido e confiável para a empresa.

Alguns criminosos podem até mesmo ser ex-funcionários recentemente demitidos querendo se vingar do antigo empregador.

Eles tornam sua identidade obscura, mas suficientemente crível para evitar perguntas. Isso exige um pouco de pesquisa por parte do golpista e envolve alto risco. Então, se alguém tenta esse método, eles identificaram um claro potencial para uma recompensa altamente valiosa se tiverem sucesso.

Ataques de pretexto

O *pretexting* utiliza uma identidade enganadora como "pretexto" para estabelecer confiança, como se passar diretamente por um fornecedor ou um funcionário do local. Essa abordagem exige que os golpistas interajam de forma mais proativa com você. A exploração ocorre uma vez que te convenceram de que são legítimos.

Golpes de *tailgating*

Tailgating, ou *piggybacking,* é o ato de seguir um membro autorizado da equipe em uma área de acesso restrito. Os agressores podem se aproveitar da cortesia social para fazer com que você segure a porta para eles ou convencê-lo(a) de que eles também estão autorizados a estar na área. O pretexto também pode desempenhar um papel aqui.

Golpes *quid pro quo*

Quid pro quo é um termo que significa aproximadamente "**toma lá, dá cá**", o que no contexto do *phishing* significa uma troca das suas informações pessoais por alguma recompensa ou outra compensação. Sorteios ou ofertas para participar de estudos de pesquisa podem expor você a esse tipo de golpe.

A exploração se dá ao te deixar animado por algo valioso que requer um baixo investimento de sua parte. No entanto, o atacante simplesmente pega seus dados sem nenhuma recompensa para você.

Ataques de *DNS spoofing* e *cache poisoning*

A ***DNS spoofing*** manipula seu navegador e servidores *web* para visitar *sites* maliciosos quando você insere uma URL legítima. Uma vez infectado por esse *exploit*, o redirecionamento continuará a menos que seja feita uma limpeza dos dados de roteamento incorretos nos sistemas envolvidos.

Os **ataques de *DNS cache poisoning*** infectam especificamente o seu dispositivo com instruções de roteamento para que a URL legítima ou várias URLs se conectem a *sites* fraudulentos.

Ataques de *scareware*

O ***scareware*** é uma forma de *malware* usada para te assustar e fazer você agir. Esse *malware* enganador utiliza advertências alarmantes que relatam infecções falsas por *malware* ou afirmam que uma de suas contas foi comprometida.

Desse modo, o *scareware* induz você a comprar *software* fraudulento de cibersegurança ou divulgar detalhes privados como suas credenciais de conta.

Ataques *watering hole*

Ataques ***watering hole*** infectam páginas da *web* populares com *malware* para afetar muitos usuários de uma só vez. É necessário um planejamento cuidadoso por parte do atacante para encontrar vulnerabilidades em *sites* específicos. Eles procuram vulnerabilidades existentes que não são conhecidas e corrigidas - tais fraquezas são chamadas de *exploits* de dia zero.

Em outras ocasiões, eles podem perceber que um *site* não atualizou sua infraestrutura para corrigir problemas conhecidos. Os proprietários de *sites* podem optar por atrasar as atualizações de *software* para manterem versões de *software* que eles sabem que estão estáveis. Eles mudarão assim que a nova versão tiver um histórico comprovado de estabilidade do sistema. Os *hackers* abusam desse comportamento para atacar vulnerabilidades recentemente corrigidas.

Métodos incomuns de Engenharia Social

Em alguns casos, os criminosos virtuais usam métodos complexos para realizar os ataques virtuais, como:

Phishing baseado em fax

Quando os clientes de um banco recebem um *e-mail* falso que alega ser do banco, pedindo a confirmação de seus códigos de acesso. Porém, o método de confirmação não ocorre pelo caminho habitual do *e-mail*/Internet.

Em vez disso, é solicitado que o cliente imprima o formulário contido no *e-mail*, preencha as informações e o envie por fax para o telefone do criminoso.

Distribuição tradicional de *malware* por correio

No Japão, cibercriminosos utilizaram o serviço de entrega em domicílio para distribuir CDs infectados com um *spyware* Cavalo de Tróia.

Os discos eram enviados aos clientes de um banco japonês.

Os endereços dos clientes foram roubados previamente da base de dados do banco.

Exemplos de ataques de Engenharia Social

Os ataques de *malware* merecem um foco especial, pois são comuns e têm efeitos prolongados.

Quando os criadores de *malware* usam técnicas de Engenharia Social, tentam induzir usuários desavisados a abrirem um arquivo infectado ou um *link* para um *site* infectado. Muitos *worms* de *e-mail* e outros tipos de *malware* usam esses métodos. Sem um pacote de *software* de segurança abrangente para seus dispositivos móveis e de *desktop*, você provavelmente está exposto à infecção.

Ataques de *worm*

O criminoso virtual tenta atrair a atenção do usuário para o *link* ou arquivo infectado para o usuário clicar nele.

Exemplos de ataque

worm Love Letter

Sobrecarregou servidores de *e-mails* de diversas empresas em 2000. As vítimas receberam um *e-mail* que as convidava a abrir a carta de amor anexada. Quando abriam o arquivo anexo, o *worm* se autocopiava para todos os contatos do catálogo de endereços da vítima. Este *worm* ainda é considerado um dos mais devastadores em termos do prejuízo financeiro causado.

worm de e-mail Mydoom

Surgiu na Internet em janeiro de 2004, usava textos que imitavam mensagens técnicas enviadas pelo servidor de *e-mail*.

worm Swen

Passava-se por uma mensagem enviada pela *Microsoft*. Ele alegava que o anexo era uma correção que removeria vulnerabilidades do *Windows*. É difícil de acreditar que tantas pessoas o levaram a sério e tentaram instalar a falsa "correção" que, na verdade, era um *worm*.

Canais de distribuição de *links* de *malware*

Os *links* para *sites* infectados podem ser enviados por *e-mail*, ICQ e outros sistemas de mensagens instantâneas, ou até em salas de bate-papo IRC na Internet. Frequentemente, os vírus de dispositivos móveis são enviados por mensagens SMS.

Seja qual for o método de envio, a mensagem normalmente contém palavras atraentes ou intrigantes, que motivam o usuário desavisado a clicar no *link*.

Esse método de invasão do sistema pode permitir que o *malware* passe pelos filtros antivírus do servidor de *e-mail*.

Ataques de rede *peer-to-peer* (P2P)

As redes P2P também são usadas para distribuir *malware*. Um *worm* ou Cavalo de Tróia aparece na rede P2P, mas recebe um nome que chama atenção e leva os usuários a baixarem e a abrirem o arquivo.

Exemplos

AIM & AOL Password Hacker.exe

Microsoft CD Key Generator.exe

PornStar3D.exe

Emulador Play Station crack.exe

Envergonhando usuários infectados a ponto de não denunciar um ataque

Em alguns casos, os criadores e distribuidores de *malware* tentam reduzir a probabilidade de as vítimas denunciarem uma infecção.

As vítimas podem responder a uma oferta falsa de aplicativo gratuito ou um guia que promete benefícios ilegais.

Exemplos

- **Acesso gratuito à Internet ou à comunicação por dispositivos móveis.**
- **A oportunidade de baixar um gerador de números de cartão de crédito.**
- **Método para aumentar o saldo da conta online da vítima.**

Nesses casos, quando se descobre que o *download* é um Cavalo de Tróia, a vítima não quer divulgar suas intenções ilícitas. Portanto, é provável que ela não denuncie a infecção para as autoridades legais.

Um exemplo dessa técnica foi o Cavalo de Tróia enviado para endereços de *e-mail* extraídos de um *site* de recrutamento. As pessoas registradas no *site* recebiam falsas ofertas de trabalho que continham o Cavalo de Tróia.

O ataque visou principalmente endereços de *e-mail* corporativos. Os criminosos sabiam que os funcionários que recebessem o Cavalo de Tróia não contariam a seus empregadores que haviam sido infectados enquanto procuravam outros empregos.

Como evitar ataques de Engenharia Social?

Defender-se contra Engenharia Social requer que você se conscientize. **Sempre diminua a velocidade e pense antes de fazer ou responder qualquer coisa.**

Quem ataca espera que você aja antes de considerar os riscos, o que significa que você deve fazer o contrário.

Para ajudar, aqui estão **algumas perguntas que podem ser feitas ao suspeitar de um ataque.**

Minhas emoções estão intensificadas?

Quando se está especialmente curioso, com medo ou animado, é menos provável que se avalie as consequências das ações.

Na verdade, provavelmente você não vai considerar a legitimidade da situação apresentada a você.

Se seu estado emocional estiver intensificado, considere isso um sinal de alerta.

Esta mensagem veio de um remetente legítimo?

Ao receber uma mensagem suspeita, verifique cuidadosamente os endereços de *e-mail* e os perfis de mídia social. Pode haver caracteres que imitam outros, como **"torn@example.com"** em vez de ***"tom@example.com"***.

Perfis falsos em redes sociais que duplicam a foto e outros detalhes do seu amigo também são comuns.

Meu amigo realmente me enviou esta mensagem?

É sempre bom perguntar ao remetente se foi ele o verdadeiro remetente da mensagem em questão. Seja um colega de trabalho ou outra pessoa em sua vida, pergunte pessoalmente ou por telefone, se possível.

A pessoa pode estar sendo *hackeada* e não sabe, ou alguém pode estar imitando sua conta.

O *site* em que estou tem detalhes estranhos?

Irregularidades na URL, baixa qualidade de imagem, logotipos antigos ou incorretos da empresa e erros de digitação na página podem ser sinais de alerta de um *site* fraudulento.

Se você entrar em um *site* falso, saia imediatamente.

Essa oferta parece boa demais para ser verdade?

No caso de brindes ou outros métodos de segmentação, as ofertas são uma forte motivação para impulsionar um ataque de Engenharia Social.

Você deve considerar por que alguém está oferecendo algo de valor com pouco ganho para si mesmo. Esteja sempre atento, pois até mesmo dados básicos como seu endereço de *e-mail* podem ser coletados e vendidos para anunciantes indesejáveis.

Anexos ou *links* suspeitos

Se um *link* ou nome de arquivo parecer vago ou estranho em uma mensagem, reconsidere a autenticidade de toda a comunicação.

Além disso, considere se a mensagem foi enviada em um contexto estranho, momento inadequado ou levanta outras suspeitas.

Essa pessoa pode comprovar sua identidade?

Se você não conseguir fazer com que essa pessoa verifique sua identidade na organização da qual ela afirma fazer parte, não conceda a ela o acesso que está solicitando.

Isso se aplica tanto pessoalmente quanto *online*, pois violações físicas exigem que você ignore a identidade do atacante.

Como prevenir ataques de Engenharia Social?

Além de detectar um ataque, você também pode ser proativo em relação à sua privacidade e segurança. Saber como prevenir ataques de Engenharia Social é incrivelmente importante para todos os usuários de dispositivos móveis e computadores.

Aqui estão algumas maneiras importantes de se proteger contra todos os tipos de ataques cibernéticos.

Crie hábitos de comunicação segura e gerenciamento de conta[10]

A comunicação *online* é ocasião onde você está especialmente vulnerável.

As mídias sociais, *e-mails* e mensagens de texto são alvos comuns, mas você também deve considerar as interações pessoais.

10 Item 5 da Política de Controle de Acesso da Política de Segurança da Informação (PSI).

Nunca clique em *links* em nenhum *e-mail* ou mensagem

Você deve sempre digitar manualmente uma URL na barra de endereço, independentemente do remetente.

No entanto, dê um passo a mais e investigue para encontrar uma versão oficial da URL em questão.

Nunca confie em qualquer URL que você não tenha verificado como oficial ou legítima.

Use autenticação multifator

As contas *online* são muito mais seguras quando são usados mais do que apenas uma senha para protegê-las.

A autenticação multifator adiciona camadas extras para verificar sua identidade ao fazer *login* em uma conta.

Esses "fatores" podem incluir **biometria** como impressão digital ou reconhecimento facial, ou senhas temporárias enviadas por mensagem de texto.

Use senhas fortes (e um gerenciador de senhas)

Cada uma das suas senhas deve ser única e complexa. Tente sempre usar caracteres de diversos tipos, incluindo maiúsculas, números e símbolos.

Além disso, provavelmente você deveria optar por senhas mais longas quando possível.

Para ajudá-lo a gerenciar todas as suas senhas personalizadas, você pode querer usar um *gerenciador de senhas* para armazená-las e lembrá-las com segurança.

Seja muito cauteloso ao construir amizades apenas *online*

Embora a internet possa ser uma ótima maneira de se conectar com pessoas ao redor do mundo, essa é uma forma comum de ataques de Engenharia Social.

Observe sinais e alertas que indicam manipulação ou um claro abuso de confiança.

Evite compartilhar nomes de suas escolas, animais de estimação, local de nascimento ou outros detalhes pessoais

Você pode estar inadvertidamente expondo respostas às suas perguntas de segurança ou partes da sua senha.

Se você configurar suas perguntas de segurança para poder lembrar delas, mas elas são imprecisas, dificultará que um criminoso invada a sua conta.

Se o seu primeiro carro foi um "Toyota", escrever uma mentira como "carro de palhaço" no lugar poderia confundir totalmente quaisquer *hackers* curiosos.

Tenha hábitos seguros de uso da rede

Redes *online* com problemas de segurança podem ser outro ponto de vulnerabilidade explorado para pesquisa de antecedentes.

Para evitar que seus dados sejam usados contra você, tome medidas de proteção em qualquer rede na qual você esteja conectado.

Nunca permita que estranhos se conectem à sua rede *wi-fi* principal

Em casa ou no local de trabalho, o acesso a uma conexão *wi-fi* para convidados deve ser disponibilizado.

Isso permite que sua conexão principal criptografada e protegida por senha permaneça segura e livre de interceptações.

Se alguém decidir "escutar secretamente" para obter informações, não será capaz de acessar a atividade que você e outros desejam manter privada.

Use uma VPN

Caso alguém na sua rede principal — com fio, sem fio ou até mesmo celular — encontre uma maneira de interceptar o tráfego, uma **rede virtual privada (VPN)** pode mantê-lo afastado.

VPNs são serviços que oferecem a você um "túnel" privado e criptografado em qualquer conexão à internet que você usa. Sua conexão não só está protegida de olhares indesejados, mas também seus dados são anonimizados, de forma que não podem ser rastreados até você através de *cookies* ou outros meios.

Mantenha todos os dispositivos e serviços conectados à rede seguros

Muitas pessoas estão cientes das práticas de segurança na internet para dispositivos móveis e computadores tradicionais.

No entanto, garantir a segurança da sua rede, assim como de todos os seus dispositivos inteligentes e serviços em nuvem é tão importante quanto.

Não deixe de proteger dispositivos comumente negligenciados, como sistemas de informação e entretenimento do carro e roteadores de rede doméstica.

Violações de dados nesses dispositivos podem alimentar a personalização para um golpe de Engenharia Social.

Hábitos seguros de uso de dispositivos

Manter seguros seus dispositivos em si é tão importante quanto todos os outros comportamentos digitais. Proteja seu celular, *tablet* e outros dispositivos de computador. Seguem as dicas.

Utilize um *software* abrangente de segurança na *internet*

Caso as táticas sociais sejam bem-sucedidas, as infecções por *malware* são um resultado comum.

Para combater *rootkits*, cavalos de Tróia e outros *bots*, é importante empregar uma **solução de segurança de *Internet*** de alta qualidade, capaz de eliminar infecções e rastrear sua origem.

Nunca deixe seus dispositivos desprotegidos em público

Sempre bloqueie seu computador e dispositivos móveis, especialmente no trabalho.

Ao usar seus dispositivos em espaços públicos como aeroportos e cafeterias, sempre os mantenha em sua posse.

Mantenha seus *softwares* atualizados assim que estiverem disponíveis

As atualizações imediatas fornecem correções essenciais de segurança para o seu *software*.

Quando você pula ou atrasa as atualizações do seu sistema operacional ou aplicativos, está deixando brechas de segurança conhecidas expostas para os *hackers* atacarem.

Como eles sabem que esse é o comportamento de muitos usuários de computador e celular, você se torna um alvo principal para ataques de *malware* com Engenharia Social.

Verifique se há violações de dados conhecidas em suas contas *online*

Serviços como o ***Kaspersky Premium*** monitoram ativamente violações de dados novas e existentes para seus endereços de *e-mail*. Se as suas contas estiverem incluídas nos dados comprometidos, você receberá uma notificação juntamente com conselhos sobre como tomar providências.

A proteção contra Engenharia Social começa com a educação.

Se todos os usuários estiverem conscientes das ameaças, nossa segurança como sociedade melhorará.

Não esqueça de aumentar a conscientização sobre esses riscos compartilhando o que você aprendeu com colegas de trabalho, família e amigos.

O que é um ataque de negação de serviço?

Um ataque de Negação de Serviço (*DoS*) é um tipo de ataque cibernético em que um ator malicioso objetiva 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.

Como funciona o ataque *DDoS*?

O foco de um ataque *DoS* é saturar em excesso a capacidade de uma máquina visada, resultando em uma negação de serviço para pedidos adicionais.

Os vários vetores de ataques *DoS* podem ser agrupados por suas semelhanças.

Categorias de ataques de *DoS*

Ataques de estouro de *buffer*

Ataques de inundação

Um tipo de ataque em que um **estouro de *buffer*** de memória pode fazer com que uma máquina consuma todo o espaço, a memória ou o tempo de CPU disponível no disco rígido.

Essa forma de uso indevido frequentemente acarreta comportamento lento, falhas no sistema ou outros comportamentos prejudiciais ao servidor, resultando em negação de serviço.

Ao saturar um servidor visado com uma enorme quantidade de pacotes, um ator malicioso pode saturar demais a capacidade do servidor, resultando em negação de serviço.[11]

Para que a maioria dos ataques de inundação *DoS* tenha sucesso, o ator malicioso deve ter mais largura de banda disponível do que o alvo.

Um ataque distribuído de negação de serviço *(DDoS*) é um tipo de ataque *DoS* que se origina em muitas fontes distribuídas, tais como um **ataque *DDoS de botnet***.

11 Disponível em: https://www.ibm.com/think/topics/phishing. Acesso em: 26 dez. 2024.

Análise de Riscos e Vulnerabilidades Internas com Implicações na Lei Geral de Proteção de Dados (LGPD) no Setor Público

A especificidade da atuação dos órgãos públicos, caracterizada pelo tratamento de um volume significativo de dados pessoais sensíveis e pela sua missão de servir à sociedade, eleva a criticidade da análise de riscos e vulnerabilidades internas com potencial para violar a Lei Geral de Proteção de Dados (LGPD). A ocorrência de incidentes de segurança originados no próprio ambiente interno pode acarretar consequências particularmente graves, minando a confiança pública e comprometendo a prestação de serviços essenciais.

A teoria da segurança da informação, em observância ao Plano de Segurança da Informação,[12] aplicada ao contexto do setor público identifica diversas modalidades de ameaças internas que podem levar à violação da LGPD.

Exemplos de riscos internos identificados

Acesso indevido facilitado pela amplitude de funções

Servidores públicos, em virtude da natureza multifacetada de suas atribuições, podem possuir acesso a uma vasta gama de dados pessoais. A falta de separação de funções e a ausência de controles de acesso estritos podem facilitar o acesso indevido a informações que não são necessárias para o desempenho de suas tarefas.

Vazamento de dados por negligência ou falta de conscientização

A ausência de treinamento adequado sobre as disposições da LGPD e as melhores práticas de segurança da informação pode levar servidores a práticas negligentes. Isso inclui o compartilhamento inadequado de dados por e-mail, o armazenamento inseguro de informações em dispositivos pessoais ou o descarte inadequado de documentos contendo dados pessoais.

12 Disponível em: https://www.ibm.com/think/topics/phishing. Acesso em: 6 jan 2024.

Uso indevido de sistemas e recursos para fins pessoais

A utilização de sistemas e recursos de tecnologia da informação do órgão público para fins particulares pode expor dados pessoais a riscos, seja pela conexão a redes não seguras, pela instalação de softwares não autorizados ou pela possibilidade de acesso por terceiros.

Aproveitamento de privilégios para obtenção de vantagem indevida

Em cenários mais graves, servidores com altos níveis de acesso podem utilizar seus privilégios para obter informações confidenciais para ganho pessoal, favorecimento de terceiros ou até mesmo para atividades ilícitas.

Ataques de Engenharia Social direcionados a servidores

Agentes maliciosos podem direcionar ataques de engenharia social especificamente a servidores públicos, explorando a confiança, a falta de conhecimento técnico ou a vulnerabilidade emocional para obter acesso a sistemas ou informações confidenciais.

Descontentamento e ações maliciosas de servidores

Servidores insatisfeitos ou com intenções maliciosas podem deliberadamente buscar comprometer a integridade, a confidencialidade ou a disponibilidade dos dados pessoais sob a responsabilidade do órgão público.

Boas práticas em Proteção de Dados Pessoais

L G P D

Ze**L**ar para que documentos do trabalho e computadores não fiquem à vista.

Utilizar a fra**G**mentadora ou similar para descarte de documentos, CDs/DVDs que contenham dados pessoais.

Não deixar visíveis informações que **P**ossibilitam acesso, como login e senha.

Bloquear a tela do computador quando não estiver na estação **D**e trabalho.

LGPD

Analisar a possibi**L**idade do órgão/entidade organizar Comitê de Proteção de Dados Pessoais.

Dentro da área, averi**G**uar se todos podem ter acesso aos dados pessoais tratados ou se os dados devem ser restritos às pessoas autorizadas.

Realizar o mapeamento dos **P**rocessos e fluxos que envolvam o tratamento dos dados pessoais.

Verificar a necessidade de controle **D**e acesso.

LGPD

Privacy by Design

A LGPD exige a implantação do *Privacy by Design,* que nada mais é do que a adoção de medidas de segurança, técnicas e administrativas, aptas a protegerem os dados pessoais, desde a fase de concepção do produto ou do serviço até a sua execução.

Glossário

- **Acesso Prejudicado ou Impossibilitado:** situação em que a capacidade de acessar sistemas, redes ou informações é comprometida ou bloqueada.
- **Acesso Não Autorizado:** acesso a um sistema, rede ou dados sem permissão.
- ***Adware*:** *software* que exibe publicidade indesejada em um dispositivo.
- ***Angler phishing:*** é uma forma de ataque de engenharia social que visa usuários de mídia social. O invasor engana suas vítimas para que forneçam informações vitais, disfarçando-se como uma fonte confiável nas redes sociais, usando contas falsas. Eles podem acessar seu banco, e-mail, criptomoedas e outras contas.
- **APWG (*Anti-Phishing Working Group*):** Grupo de Trabalho Anti-Phishing é um consórcio internacional focado em fornecer orientação e coletar dados para reduzir os riscos de fraude e roubo de identidade causados por phishing e incidentes relacionados.
- **Ataque Cibernético:** ação maliciosa em meio digital, com o objetivo de comprometer a segurança de sistemas, redes ou dados.
- **Autenticação Multifator:** método de segurança que requer mais de uma forma de identificação para acessar uma conta ou sistema.
- ***Baiting:*** é como um Cavalo de Tróia digital. Ela explora a curiosidade ou a ganância da vítima para alcançar seus objetivos.
- ***BEC (Business Email Compromise)*:** Comprometimento de e-mail comercial. É uma classe de ataques de spear phishing que tentam roubar dinheiro ou informações valiosas de uma empresa, ou organização.
- ***Botnet*:** rede de dispositivos infectados por malware, controlados remotamente por um invasor.
- ***Buffer:*** nome dado ao processo de pré-carregamento de dados na memória do computador.
- ***Cache poisoning:*** técnica avançada na qual um invasor explora o comportamento de um servidor da Web e do cache para que uma resposta HTTP prejudicial seja enviada a outros usuários.
- **Cavalo de Tróia (*Trojan*):** *malware* que se disfarça de software legítimo para realizar tarefas maliciosas.
- ***Desktop:*** é conhecido como área de trabalho, pois permite ao usuário ter acesso fácil a todos os elementos que fazem parte do sistema operativo (pastas, arquivos, atalhos, programas etc.). É uma analogia ao ambiente de trabalho físico, onde estão organizados todos os recursos necessários para a execução das tarefas.
- ***DNS (Domain Name System)*:** sistema de nomes de domínio.
- ***DNS cache poisoning:*** envenenamento de cache de *DNS* é o ato de inserir informações falsas em um *cache* de *DNS* para que as consultas de *DNS* retornem uma resposta incorreta e os usuários sejam direcionados aos sites errados.

- ***DoS (Denial of Service):*** *ataque cibernético que visa tornar um computador ou dispositivo indisponível para os usuários, utilizando um único computador para o ataque.*

- ***DDoS (Distributed Denial of Service):*** ataque *DoS* que se origina em múltiplas fontes distribuídas, como uma *botnet*.

- ***DNS spoofing*****:** ataque que usa registros de Nome de Domínio alterados para redirecionar o tráfego para um site fraudulento.

- ***EAC (Email Account Compromise)*****:** comprometimento de conta de e-mail. O golpista compromete a conta de e-mail de um funcionário de nível inferior e usa a conta para enviar faturas fraudulentas a fornecedores, instruir outros funcionários a fazerem pagamentos fraudulentos ou solicitarem acesso a dados confidenciais.

- ***EDR (Endpoint Detection and Response)*****:** soluções de detecção e resposta de *endpoint*.

- **Engenharia Social:** técnica de manipulação que explora erros humanos para obter informações, acessos ou coisas de valor.

- ***Exploit:*** *software*, um bloco de dados ou uma sequência de comandos que se aproveita de um *bug* ou vulnerabilidade em um aplicativo ou sistema para causar a ocorrência de comportamentos não intencionais ou não antecipados.

- ***Firewall*****:** sistema de segurança que monitora e controla o tráfego de rede, bloqueando acessos não autorizados.

- ***FTC (Federal Trade Comission)*****:** Comissão Federal de Comércio dos EUA.

- ***Hakeada:*** burlar a segurança de um sistema computacional, buscando acessar ilegalmente, sem a permissão do dono, um computador ou sistema computacional e informático: *hackear* as contas de uma empresa buscando os dados pessoais dos funcionários.

- **IA (Inteligência Artificial):** o *phishing* de IA usa ferramentas de inteligência artificial (IA) generativas para criar mensagens de *phishing*.

- **IRS (*Internal Revenue Service):*** serviço de receita do Governo Federal dos Estados Unidos. A agência faz parte do Departamento do Tesouro, sob a direção imediata do *Commissioner of Internal Revenue.*

- ***Kaspersky*** **premium:** assinatura que oferece proteção contra ameaças digitais, como vírus, *malwares, ransomwares*, aplicativos de espionagem e outros. Ele também inclui serviços premium, como suporte remoto de TI e proteção de identidade.

- **LGPD:** Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, de 14 de agosto de 2018: dispõe sobre o tratamento de dados pessoais, em meios físicos e digitais, realizado por pessoa natural ou jurídica de direito público ou privado, com o objetivo de proteger os dados pessoais dos titulares.

- ***Link:*** elemento de hipermídia formado por um trecho de texto em destaque ou por um elemento gráfico que, ao ser acionado, provoca a exibição de novo hiperdocumento.

- ***Malware*****:** termo genérico para software malicioso que pode prejudicar dispositivos, serviços ou redes.

- **O*nline:*** que se pode acessar pelo computador. Que está numa conexão ou na internet no exato momento em que acessa; conectado.

- ***Peer-to-peer (P2P):*** *ti*po de rede distribuída na qual os computadores conectados ao sistema funcionam também como servidores. Já na economia, em especial no universo das criptomoedas, o P2P é um tipo de transação que ocorre diretamente entre os usuários, sem a intermediação de uma terceira parte.

- ***Phishing:*** técnica de manipulação que usa comunicações fraudulentas para induzir as pessoas a compartilhar dados confidenciais.

- ***Pretexting:*** uso de história fabricada, ou pretexto, para ganhar a confiança de uma vítima e enganá-la ou manipulá-la para compartilhar informações confidenciais, baixar *malware*, enviar dinheiro para criminosos ou prejudicar a si mesma ou à organização para a qual trabalha.

- ***Quid pro quo*****:** ataque digital muito popular entre os criminosos. Esse golpe pode levar à divulgação de informações pessoais ou à violação da segurança cibernética.

- ***Quishing:*** *phishing* por meio de códigos QR falsos.

- ***Ransomware*****:** m*alware* que impede o acesso a dados da vítima, exigindo um resgate para restaurar o acesso.

- ***Rootkits:*** *malware* projetado para dar aos *hackers* acesso e controle sobre um dispositivo.

- ***Tailgating*****:** técnica de engenharia social utilizada por indivíduos que procuram obter acesso não autorizado a áreas seguras, seguindo de perto uma pessoa autorizada. Esta tática explora a cortesia humana, permitindo que o infiltrador ganhe acesso sem a devida autenticação.

- ***Scareware*****:** um tipo de golpe de engenharia social que usa o medo para enganar as pessoas para que elas façam *download* de um *malware*, perdendo dinheiro ou entregando dados pessoais.

- ***Smishing:*** *phishing* por SMS (mensagens de texto).

- ***Spear phishing:*** é um tipo de ataque de *phishing* que tem como alvo um indivíduo ou grupo específico de indivíduos dentro de uma organização, e tenta enganá-los para divulgar informações confidenciais, fazer o *download* de malware ou enviar inconscientemente nossos pagamentos autorizados ao invasor.

- ***Spyware*****:** s*oftware* que coleta informações do dispositivo e envia para terceiros sem consentimento do usuário.

- **Vírus:** *malware* que infecta programas e arquivos, propagando-se ao fazer cópias de si mesmos em outros softwares.

- ***Vishing:*** *phishing* por voz (chamada telefônica).

- ***VPN (Virtual Private Network)*****:** rede virtual privada que oferece um "túnel" privado e criptografado em qualquer conexão à internet.

- **W*atering hole:*** a exploração de segurança na qual o invasor busca comprometer um grupo específico de usuários finais, infectando *sites* que os membros do grupo costumam visitar. O objetivo é infectar o computador de um usuário alvo e obter acesso à rede no local de trabalho do alvo.

- ***Whaling:*** é um método que criminosos virtuais usam para se disfarçar como se fosse um participante de alto escalão de uma organização e atingir diretamente outras pessoas importantes, visando roubar dinheiro e informações sigilosas ou obter acesso a seus sistemas de computadores para fins criminosos.

- ***Worm:*** *malware* que se propaga automaticamente, sem ação do usuário, acessando listas de contato e enviando mensagens.

- ***Worm de e-mail Mydoom:*** verme informático que infecta o sistema operativo Microsoft Windows. Ele foi o primeiro *worm* a infectar através de e-mail.

- ***Worm love letter:*** conhecido como ILOVEYOU ou Love Bug, era um programa malicioso que se espalhava por e-mail. O *worm* danificava computadores e enviava uma cópia de si mesmo para os contatos do usuário.

- ***Worm Swen:*** vírus de *worms* muito perigoso que se espalha pela *Internet* via e-mail (na forma de um anexo de arquivo infectado).

Bibliografia

AKAMAI. **O que é *ransomware*?**. Disponível em: https://www.akamai.com/pt/glossary/what-is-ransomware#:~:text=Entendendo%20o%20ransomware,global%20e%20organiza%C3%A7%C3%B5es%20de%20sa%C3%BAde. Acesso em: 10 dez. 2024.

IBM. ***What is phishing?***. Disponível em: https://www.ibm.com/think/topics/phishing. Acesso em: 15 dez. 2024.

___. **O que é *ransomware*?**. https://www.ibm.com/br-pt/topics/ransomware#:~:text=O%20ransomware%20%C3%A9%20um%20tipo,pague%20um%20resgate%20ao%20invasor. Acesso em: 15 dez. 2024.

CLOUDFLARE. **O que é um ataque de negação de serviço *(DoS)*?**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/meus-dados-vazaram-e-agora. Acesso em: 21 dez. 2024.

GEEKSFORGEEKS. **O que é *Malware* e seus tipos?**. Disponível em: https://www.geeksforgeeks.org/malware-and-its-types/. Acesso em: 10 dez. 2024.

KASPERSKY. ***Ransomware*: definição, prevenção e remoção**. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware. Acesso em: 11 dez. 2024.

PICPAY. **Vírus no celular: aprenda a identificar e eliminar *malwares***. https://blog.picpay.com/virus-no-celular/. Acesso em: 23 dez. 2024.

UNTANGLE BRASIL. **Como identificar e responder a incidentes de segurança**. Disponível em: https://www.untanglebrasil.com.br/como-identificar-e-responder-a-incidentes-de-seguranca/. Acesso em: 11 dez. 2024.

PGE
Mato Grosso do Sul

Procuradoria-Geral
do Estado

UPD - Unidade de Proteção de Dados Pessoais

(67) 3318-2607

encarregadolgpd@pge.ms.gov.br

Link: https://www.pge.ms.gov.br/lgpd-lei-geral-de-protecao-de-dados-pessoais/

Av. Des. José Nunes da Cunha S/N
Parque dos Poderes, Bloco IV
Campo Grande - MS
CEP: 79031-310