Boas Práticas em Segurança da Informação

Julho de 2023

Elaboração: Governança de Segurança da Informação

Classificação: Pública

Código: POL SI 03

Índice

1. Introdução a Segurança da Informação

Você conseguiria trabalhar um dia sem e-mail? Ou então, sem se comunicar com seus colegas de trabalho via WhatsApp, sem ter acesso aos arquivos que você tem no seu computador?

Hoje em dia, existem incidentes cibernéticos que podem tornar recursos digitais indisponíveis, como um "sistema fora do ar", um banco de dados exposto com informações confidenciais de clientes, ou até arquivos de trabalho deletados.

A Segurança da Informação é a principal responsável para que esses serviços digitais funcionem, desde sua disponibilidade até a sua integridade e confidencialidade dos dados e informações de seus usuários.

Em contrapartida, estima-se que o cibercrime gere um prejuízo de 6 trilhões bilhões de dólares a nível mundial, cerca de 4 vezes o PIB do Brasil. Os ataques cibernéticos prosseguem crescendo a um ritmo alarmante, em volume, em sofisticação e impacto. Nessa era de crimes cibernéticos excessivos, a necessidade de se proteger contra os ataques avançados é mais importante do que nunca.

1.1. O que fazer para frear o cibercrime?

Além de investimentos em tecnologia mais eficientes e processos de segurança, é preciso que as pessoas estejam conscientizadas das boas práticas de Segurança da Informação para que a efetividade dos ataques cibernéticos seja neutralizada. Por isso, abordaremos algumas dicas neste documento.

2. Autenticação Segura

O primeiro passo para proteger nossas credenciais (login e senha) de ataques de bruteforce (software utilizado por cibercriminosos para descobrir uma senha) é criando uma "**senha forte**", que precisa seguir os seguintes requisitos:

- Letras maiúsculas e minúsculas
- Números
- Caractere especial (%@#$&)
- No mínimo 12 dígitos
- Não deve ser igual a alguma senha já utilizada

Para te apoiar a criar senhas fortes, temos o seguinte método, que não precisa de tanta criatividade ou imaginação:

1. **Escolha uma palavra ou frase**, algo que você goste ou almeja. Como exemplo, vou usar a palavra "**sexta-feira**".
2. **Troque alguma das letras por números e símbolos**, assim a nossa simples "sexta-feira" se transforma em "**$ext@ -f&1r4**".
3. **Quanto mais longa for a senha, mais forte será**. Então de "sexta-feira" poderíamos evoluir para "eu adoro sexta-feira", ou melhor, "**&u @d0r0 $ext4-f&ir4**".

Você deve estar se perguntando: **Como vou decorar tantas senhas?**

Para não depender só da memória e da criatividade, existem programas chamados **Gerenciadores de Senhas** que possuem recurso de **criar, salvar e compartilhar as suas senhas de forma segura**.

Os gerenciadores **funcionam como um cofre** através de plug-in para navegadores e aplicativo mobile, e a aplicação **criptografa todas as suas senhas** e reconhece apenas os dispositivos autorizados a acessá-la.

Dessa forma, mesmo que alguém descubra a sua senha mestra, essa pessoa não terá acesso as suas senhas.
Sugestão de Gerenciadores de Senhas:

- 1Password
- Dashlane
- LastPass

Além de senhas fortes e gerenciadores, há alguns outros cuidados que devemos ter com nossas credenciais como:

2.1. Troque sua senha com regularidade

Às vezes pode ser difícil saber se nossos dados estão em alguma base vazada. Então, trocar a senha com regularidade pode servir de prevenção para esse tipo de caso. Podemos tomar como base uma regularidade de 3 em 3 meses para atualizar as senhas.

Se você souber que algum serviço ou empresa em que você tem cadastro teve um vazamento de informação, troque sua senha imediatamente.

2.2. Não anote senha em post-it, cadernos ou arquivos digitais (documentos de texto, planilhas ou apresentação)

Nenhum desses métodos citados possuem uma confiabilidade alta para armazenar suas senhas de forma segura. Para salvar as suas senhas, utilize sempre os gerenciadores de senhas.

2.3. Não compartilhar seu e-mail e senha

Ao compartilhar algum tipo de acesso que você tenha, sempre há risco de vazamento a terceiros não autorizados ou comprometimento de acesso por armazenamento inadequado.

2.4. Faça utilização de autenticação em dois fatores

A autenticação de dois fatores é uma camada extra de proteção que pode ser ativada em contas online. Ao ativar a verificação em duas etapas, o usuário precisa fornecer uma segunda informação após inserir as credenciais, e só então terá acesso à conta.
Cada Plataforma oferece diferentes métodos de verificação, que podem compreender códigos SMS, dispositivos de token ou biometria, por exemplo.

A principal ideia por trás da autenticação de duas etapas é dificultar o acesso à conta. Mesmo que a senha seja hackeada ou o telefone roubado, dificilmente outro usuário conseguirá entrar nos seus perfis, porque ele não terá informações do Segundo fator.

A forma mais segura é utilizar aplicativos de MFA, pois são gerados códigos aleatórios válidos por poucos segundos para se autenticar com sucesso na conta. Alguns exemplos de aplicativos MFA:

- Microsoft Authenticator;
- Authy;
- Google Authenticator.

Obs.: Para não cair em golpes, é importante nunca compartilhar o código recebido com terceiros. É comum que criminosos entrem em contato com vítimas alegando motivos falsos para solicitar um código enviado por SMS.

3. Navegação Segura

Para começar a falar sobre navegação segura, vamos iniciar pela sua conectividade à Internet.

3.1. Introdução a Segurança da Informação

Um dos ataques mais eficazes para roubo de informações confidenciais é a partir de redes de Wi-Fi públicas presentes na maioria dos estabelecimentos comerciais, como cafeterias, restaurantes, livrarias, shoppings e aeroportos.

O cibercriminoso intercepta os dados que estão sendo trafegados naquela rede, conseguindo ter visualização clara de logins, senhas e sites que você está acessando, embora eles somente tenham êxito na coleta se algum site ou aplicativo acessado não utilizar HTTPS (protocolo que criptografa dados na Web que fica antes do “www.”).

Por garantia, **a recomendação é de se usar o 3G/4G/5G** em caso de dispositivos móveis ou, se realmente precisar entrar no Wi-Fi, **evite acessar serviços críticos**, como contas de banco e e-mail, a não ser que você tenha certeza de que o protocolo HTTPS esteja sendo usado e não receba alerta de certificado inválido.
Caso você procure ou precisar de mais privacidade para sua navegação na internet, vale a pena assinar um plano de VPN. Sugestões:

- NordVPN;
- Surfshark;
- Private Internet Access.

3.2. Aprimorando a segurança do seu navegador

3.2.1. Preste atenção no HTTPS:

Como já vimos anteriormente, o HTTPS é o protocolo que garante a criptografia da comunicação entre você e o site. Você pode vê-lo lá na barra de navegação antes do “www.”, ou em forma de ícone de cadeado.

Então fique de olho nos sites em que você está entrando. Serviços como bancos, lojas virtuais, redes sociais e sites de notícia possuem o HTTPS. Caso você entre em algum site que você conhece e que não tenha o protocolo, verifique a URL. Você pode estar entrando em algum site falso.

Vale frisar que o cadeado no site não é uma absoluta certeza de que o site é legítimo. O HTTPS serve para atestar credibilidade de que os dados trafegados no site são seguros, mas não é uma garantia definitiva.

3.2.2. Propagandas e Pop-ups

Uma forma de disseminar vírus pela Internet é através de pop-ups e propagandas em banners de sites. Essa prática é chamada de Adware, e você pode evitá-la desativando os pop-ups do seu navegador e instalando um plug-in (extensão) chamado Adblock. Alguns exemplos de bloqueadores de pop-ups:

- Adblock;
- Chrome;
- Firefox

3.2.3. Ative a Função navegação Segura.

Com essa funcionalidade ativada, o seu navegador irá te avisar quando você está entrando em algum site que pode ser considerado malicioso, que seja usado em golpes de *phishing* ou que seja para disseminar vírus. Como ativar a navegação segura:

- Chrome;
- Firefox;

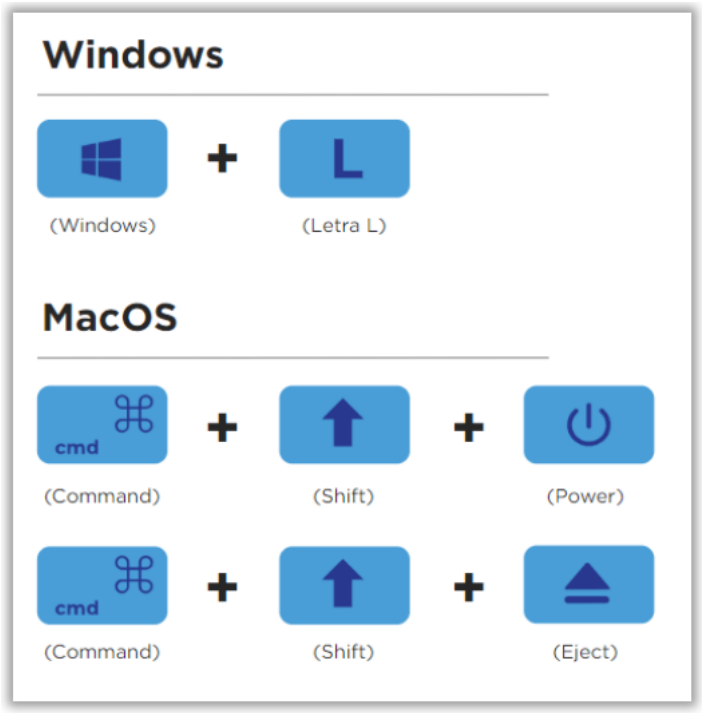
3.2.4. Zelando pela confidencialidade de suas informações

É muito comum se ausentar do computador e deixá-lo desbloqueado, porém essa prática contribui para que incidentes de vazamento de informações ocorram, pois, qualquer pessoa pode acessar uma variedade de informações de seu computador como arquivos que deveriam ser confidenciais, e-mails e conversas privadas, e até suas credenciais de serviços online. Além disso, podem possivelmente usar seu acesso de modo indevido, como por exemplo, enviar um e-mail ou compartilhar dados sensíveis em seu nome.

Por isso, ao se ausentar do seu computador, seja por qualquer motivo (ir ao banheiro, almoçar, ir para uma reunião), lembre-se de bloquear a máquina:

Em computadores nos quais o sistema operacional é o **Windows**, o atalho para bloquear a máquina é o botão do “**Windows + L**”, já em sistemas da **Apple** use o atalho “***Control* + *Shift* + *Power***”.

No caso de tablets e **dispositivos móveis**, sempre mantenha travado por senha, e reduza o tempo de bloqueio por inatividades jamais deixe desbloqueado enquanto estiver distante.



4. Engenharia Social

Engenharia Social é um conjunto de técnicas utilizadas por cibercriminosos que **consistem em persuadir e manipular a vítima** através da curiosidade, da ignorância e de um senso de urgência para que ela **execute certas ações ou forneça informações** que os permitam atingir seus objetivos.

O golpe do e-mail falso, também conhecido como *phishing* é altamente disseminado na internet. Consiste no envio de **comunicações fraudulentas** muito parecidas com as comunicações usadas por empresas reais, com o intuito de roubar credenciais de suas vítimas, informações sensíveis e cartões de crédito.

Para além de fraudes financeiras, *phishing* é uma boa porta de entrada para incidentes cibernéticos maiores.
Por exemplo, se a vítima submete suas credenciais corporativas ou baixa um arquivo malicioso, o cibercriminoso consegue uma brecha para invadir o ambiente digital da empresa, conseguindo infectar a rede com *Malware*s (vírus) ou então roubando dados de clientes e outras informações sensíveis.

4.1. Formas de Ataque de Engenharia Social

***Phishing*:** qualquer tipo de fraude por meios de telecomunicação (voz, sms, e-mail), que usa truques de engenharia social para obter dados privados das vítimas;

Vishing: Vishing é uma abreviação de Voice *Phishing* – uma variação de golpe aplicada por áudio;

Smishing: O termo smishing é uma combinação de "SMS" (short message services, ou mensagens de texto) e "*phishing*".

Independentemente da temática do *phishing*, há algumas **dicas bem simples de como identificar esse tipo de fraude**.

1. Confira se o e-mail **remetente da mensagem** é compatível com o utilizado pela empresa. Normalmente os cibercriminosos utilizam e-mails com erros ortográficos.

2. **Não responda ou clique em links de e-mails** que peçam informações pessoais ou financeiras.

3. **Nunca abra ou baixe arquivos anexos** de mensagens não solicitadas.

4. **Sempre verifique o link antes de abrir** (passando o mouse sobre o link abrirá uma pequena legenda com o link). Se ele possuir algum problema ortográfico ou algum encurtador de URL (bit.ly, migre.me), tenha certeza – cibercriminosos estão tentando enganá-lo com uma página falsa.

5. Ao invés de clicar nos links nos e-mails, **vá diretamente às páginas digitando o endereço em seu navegador**.

6. Ao receber um *Phishing* ou smishing, denuncie imediatamente e exclua assim que denunciado.

7. Assim que perceber algo estranho acesse o site oficial da loja ou instituição que supostamente enviou a comunicação e procure um telefone para contato.

5. Evitando Outros Incidentes Cibernéticos

No capítulo anterior abordamos dicas para evitar que você seja “fisgado” em um *phishing*, que é um tipo de ataque cibernético. Agora falaremos um pouco sobre *Malware*, o famoso vírus de computador.

Malware pode ser tanto códigos maliciosos dentro de arquivos (como planilhas, apresentação, PDF, arquivos de texto) quanto softwares nocivos, também conhecidos popularmente como “vírus de computador”. Dessa forma, podemos compreender *Malware* como **todo programa que contenha algum tipo de código malicioso**, seja um vírus, Cavalo de Troia (Trojan) ou *Spyware*.

5.1. Quais são os objetivos desse incidente?

Os objetivos por trás de um *Malware* podem ir desde alteração de dados até roubo de informações e espionar os usuários e dados que trafegam em sua rede.

5.2. Como posso evitar ser uma vítima?

*Malware*s podem infectar sua máquina através de e-mails de *phishing* ou arquivos baixados de fontes não confiáveis da internet, softwares piratas e vulnerabilidades tecnológicas ainda desconhecidas (*zero day*) de programas que você possui instalados.

Para evitar a infecção de *Malware*s tenha um antivírus instalado em seu computador e smartphone, fique de olho em *phishing*s e **não deixe as atualizações de aplicativos e sistema operacional para depois**.

Recomendamos também, que fique longe de softwares piratas e download de fontes não confiáveis.

5.3. Backup

Por último, mas não menos importante, a melhor dica de como se proteger de incidentes digitais: tenha sempre um backup. Backups são as principais formas de proteção conhecida contra extorsões digitais. Se os dados forem sequestrados por um criminoso, não é necessário pagar resgate, pois há outra cópia segura. Para isso, é só estabelecer uma rotina de backups dos arquivos mais importantes.

6. Glossário

- Bruteforce: Brute force é literalmente “força bruta”, termo utilizado para descrever um tipo de ataque onde se força a entrada em algum sistema, site, servidor, aplicativo, etc.
- Credencial: As credenciais de login são nomes de usuário e senhas gerenciados que dão acesso a vários apps.
- Criptografia: A criptografia envolve a conversão de texto simples legível por humanos em texto incompreensível, o que é conhecido como texto cifrado.
- VPN (Virtual Private Network): Significa “Rede Privada Virtual” e descreve a oportunidade de estabelecer uma conexão de rede protegida ao usar redes públicas.
- Adware: Adware, que vem da mistura das palavras inglesas advertising (publicidade) e *Malware* (software maliciosos) - *Malware* de publicidade - apresenta anúncios indesejados com o uso de métodos invasivos e potencialmente perigosos.

- Confiabilidade: A confiabilidade que apontamos nesse artigo, refere-se ao CID que é abreviação para confidencialidade, integridade e disponibilidade. Também conhecido como a tríade em Segurança da Informação.

- URL: O termo URL é a abreviação de Uniform Resource Locator, ou Localizador Uniforme de Recursos. Significa endereço web, ou seja, o texto que você digita na barra de do navegador para acessar uma determinada página ou serviço.

- *Malware*: *Malware* é um termo genérico para qualquer tipo de “malicious software” (“software malicioso”) projetado para se infiltrar no seu dispositivo sem o seu conhecimento.

- Trojan ou Cavalo de Tróia: O trojan, ou cavalo de tróia, é um *Malware* muito utilizado para invasões e roubos de dados.

- *Spyware*: É um tipo de *Malware* que tenta se esconder enquanto registra secretamente informações e rastreia suas atividades online em seus computadores ou dispositivos móveis.

genialinvestimentos.com.br