GUIA BÁSICO DE SEGURANÇA DA INFORMAÇÃO

PARA USO EXTERNO

INFORMAÇÕES

Título	Guia Básico de Segurança da Informação
Número da Versão	V2
Áreas Proprietárias da Política	Segurança da Informação
Palavras-chave	Ataque, Backup, Dados, Dispositivos, Internet, Phishing, Senha, Malware, Engenharia Social, Proteção

HISTÓRICO DE VERSÕES

#	Motivo da Alteração	Data	Autor	Departamento
1	Criação do Guia Básico de SI	26/07/2019	Thais Devides	Segurança da Informação
2	Revisão	30/07/019	Felipe Deco	Segurança da Informação

ÍNDICE

1. OBJETIVO

Este guia visa ajudar usuários que utilizam dispositivos eletrônicos a entenderem como se protegerem contra-ataques cibernéticos mais comuns e proteger suas informações, entretanto este guia não garante a proteção contra todos os tipos de ataques cibernéticos.

2. DEFINIÇÃO

Ataque Cibernético: É qualquer tentativa de expor, alterar, destruir, roubar ou obter acesso não autorizado de dados de um dispositivo eletrônico;

Backup: Uma cópia de segurança dos dados de um lugar para outro apartado;

Desktop: Estação de trabalho (computador) utilizado por um usuário;

Dispositivos eletrônico: exemplo de dispositivo eletrônico, mas não se limitando a estes: Computador, notebook, tablet, celular, HD externo, *pendrive*, etc.

3. USE SENHAS PARA PROTEGER SEUS DADOS

O uso de senhas seguras nunca foi tão importante. Os hackers estão ávidos por senhas. As violações de dados e vazamentos de senhas deixam facilmente milhares de contas vulneráveis ao acesso de criminosos cibernéticos. Uma senha forte e única para cada equipamento ou serviço pode evitar muita dor de cabeça. Mais do que uma senha forte, a combinação de fatores é a melhor forma de se manter seguro.

3.1 USANDO SENHAS FORTES

Proteja suas senhas e seus dispositivos utilizados na validação de suas transações. Uma maneira fácil e eficaz de prevenir que pessoas não autorizadas acessem seus dados.

Um gerenciador de senhas pode ajudar, é uma ferramenta que pode criar e armazenar senhas. Ele permite a gestão de uma única senha máster, onde é possível através dela acessar as demais senhas.

- Como a senha máster protege todas as outras senhas dentro do gerenciador:
- Evite senhas comuns como nomes de familiares e de animais de estimação
- Verifique se ela é forte, por exemplo, utilizar três palavras aleatórias com números e caracteres especiais se possível.

3.2 ATIVAR PROTEÇÃO POR SENHA

Certifique-se de que todos os computadores e notebooks exijam uma senha criptografada para inicializar. Ative proteção por senha, biometria ou reconhecimento facial para dispositivos móveis. Por isso, configure uma senha longa que seja difícil de adivinhar.

A maioria dos dispositivos modernos tem criptografia embutida, mas a criptografia ainda precisa ser ativada e configurada, portanto, verifique se você a configurou.

3.3 AUTENTICAÇÃO COM DOIS FATORES – 2FA

O Segundo Fator de Autenticação – 2FA (*Two Factor Authentication*) exige dois métodos diferentes para comprovar sua identidade antes que você possa acessar as informações. Pode ser um código enviado via token, via SMS, etc que deve ser inserido além da sua senha rotineira. Utilize dois fatores de autenticação (2FA) para sites com informações sensíveis, como bancos e *e-mail*, quando disponível a opção. Este procedimento aumenta a segurança, mas não evita.

3.4 SENHAS COMUNS

Evite usar senhas comuns como nomes de familiares, animais de estimação, datas comemorativas e senhas do tipo “camuflada” que possam facilitar o criminoso adivinhar como exemplo: p@ssw0rd, s3nh@

As senhas devem ser fáceis de lembrar, mas difíceis para outra pessoa adivinhar.

Mantenha sua senha segura, fazendo a troca no mínimo a cada 90 dias dos seus sistemas / aplicativos, contas bancárias ou quando suspeitar de um ataque bem-sucedido.

Lembre-se de que não se deve compartilhar login e senha dos seus aplicativos, inclusive e-mail para realizar qualquer atividade ou tarefa momentânea.

4. EVITANDO ATAQUE PHISHING

Phishing é uma forma de fraude eletrônica, caracterizada por tentativas de captura de dados pessoais[1] e/ou sensíveis[2]. Em ataques de phishing, o golpista envia *e-mails* falsos solicitando informações confidenciais (como dados bancários) ou contendo *links* para *sites* maliciosos, tentando se passar por outra pessoa ou empresa confiável.

Seja qual for o seu negócio, seja ele grande ou pequeno, você receberá ataques de phishing em algum momento, afim de roubar seus dados para vender ou por qualquer outro motivo para acessar suas informações ou da sua organização para ganhar dinheiro.

Assegure-se de que *links* que não legítimos sejam clicados. O fraudador utiliza mascaramento afim de fazer a vítima acreditar que o *link* seja verdadeiro (verifique se a ortografia e gramática estão corretas e se não possui baixa qualidade na versão do logotipo da empresa). Verifique o endereço de e-mail do remetente se é aparentemente autentico ou se está tentando se passar por alguém conhecido.

Alguns sinais óbvios de phishing:

- Desconfie sempre de descontos extraordinários, não se iluda, não dê credibilidade;
- Sempre leia com cuidado o *link* antes de clica-lo e desconfie de caracteres estranhos, e erros gramaticais como “utili**s**ando” ao invés de “utili**z**ando” e número como “1” no lugar da letra “l”. Na dúvida sempre prefira digitar ao invés de copiar ou clicar no endereço eletrônico de um *link* ou *site* para o navegador;
- *E-mails* com anexo suspeito, aguça a curiosidade ou medo de qualquer um abordando assuntos como: cancelamento, ou remoção da sua conta, assinaturas gratuitas, vulnerabilidade no computador, presentes (*gifts*), comunicado de dívidas, processos judiciais entre outros, atente-se:
- Nunca abra arquivos anexados a *e-mails* de origem não confirmada;
- Confirme a legitimidade do endereço eletrônico recebido;
- Nunca forneça suas credenciais de acesso como senha, login, número de conta, CPF, etc.

[1] **Dados pessoais** são informações de uma pessoa por meio das quais ela possa ser identificada, ou seja, qualquer informação que a identifique, como por exemplo: CPF, nome completo, RG, título de eleitor, data de nascimento, endereço, endereço eletrônico, telefone, devendo ser respeitada a sua privacidade, sigilo e confidencialidade.

[2] **Dados sensíveis** são dados pessoais que revelam a origem racial ou étnica, dados relativos à vida sexual ou orientação sexual da pessoa, a organização de caráter religioso, dado referente à saúde quando vinculado a uma pessoa natural.

5. PROTEJA-SE DE MALWARE

Você pode se proteger contra os danos causados por *malwares* (*softwares* mal-intencionados) incluindo vírus, que são programas automáticos que infectam o sistema de seu computador ou qualquer dispositivo móvel.

5.1 ANTIVÍRUS E APLICATIVOS

Utilize *software* de antivírus em todos os computadores e dispositivos eletrônico e o mantenha atualizado. Normalmente o antivírus já vem incluso no sistema operacional gratuitamente por um curto período de tempo. Mantenha-o ativado para reduzir o risco.

Evite fazer *download* de aplicativos de terceiros de fontes desconhecidas. Faça apenas *download* de *sites* aprovados e reconhecidos pelo fabricante. Esses aplicativos são verificados para fornecer um certo nível de proteção contra *malware* que pode causar danos.

5.2 ATIVE SEU FIREWALL

Ative o seu *firewall* (incluído na maioria dos sistemas operacionais) para criar uma zona segura entre sua rede e a internet.

6. MANTENDO SEUS DISPOSITIVOS MOVEIS SEGUROS

Smartphones e *notebooks* (que são usados diariamente em qualquer lugar) precisam de ainda mais proteção do que os equipamentos de *desktop*

6.1 ATIVAR A PROTEÇÃO POR SENHA E RASTREABILIDADE

Configurar dispositivos para que, quando perdidos ou roubados:

- Possam ser rastreados;
- Apagados ou bloqueados remotamente
- Insira uma senha bem elaborada, isso pode impedir que um criminoso acesse seus dados.
- Verifique seu dispositivo e ative proteção por senha, biometria ou reconhecimento facial para dispositivos móveis.

6.2 MANTER SEU DISPOSITIVO E APLICATIVOS ATUALIZADOS

Mantenha seus dispositivos (e todos os aplicativos instalados) atualizados e com a versão mais recente fornecida pelo fabricante, estás atualizações não só contém novos recursos, como também possuem atualizações de segurança crítica para corrigir alguma vulnerabilidade ou falha. Aplicar essas atualizações é uma das coisas mais importantes que você pode fazer para melhorar a segurança.

Pode-se utilizar a opção de atualização automática quando disponível e possível. Mantenha sempre seu *software* atualizado

Dispositivos que não são mais suportados por fabricantes, a sugestão é substituir com alternativas atualizadas.

6.3 NÃO SE CONECTAR A PONTOS DE ACESSO WI-FI DESCONHECIDOS

Ao enviar dados confidenciais, não se conecte a redes públicas de *wi-fi* – utilize conexões 3G ou 4G ou VPNs, uma técnica que criptografa seus dados antes de serem enviados pela *internet*. Caso conecte fique atento aos seguintes pontos que podem ser acessados pelo controlador da conexão:

- O que você está trabalhando enquanto conectado;
- Detalhes de *login* e senhas privadas que aplicativos e serviços da *web* mantêm enquanto você está conectado.

7. PREVENÇÃO A FRAUDE – ENGENHARIA SOCIAL

É um método de ataque, onde alguém consegue persuadir, tanto pessoalmente quanto por telefone ou através de *e-mails* se aproveitando da ingenuidade ou confiança da pessoa, para obter informações privilegiadas (sensíveis, sigilosas ou pessoais) que podem ser utilizadas para ter acesso não autorizado a dispositivos computacionais ou informações. O golpista se aproveita desta vulnerabilidade e obtêm informações que ele deseja.

Desta forma, apresentamos algumas dicas para evitar que você caia nesse golpe, como boa prática de segurança:

- Evite abrir anexos com extensões .zip, .scr, .exe de origem não confirmada, procedência desconhecida ou duvidosa – Sempre passe pelo antivírus antes;
- Esteja sempre com seu computador atualizado com as medidas de segurança instaladas em seu sistema operacional e *softwares* utilizados;
- Mantenha sempre o seu antivírus ativo e atualizado;
- Evite acessar sua conta de *e-mail* em computadores de uso público, pois são alvos fáceis para ações fraudulentas na *internet*;
- Fique atento com ligações que solicitem muitas informações via telefone ou *e-mails* de pessoas perguntando sobre dados pessoais e/ ou confidenciais;
- Não informar dados pessoais ou financeiros em *e-mail*, procurar sempre averiguar a veracidade da pessoa que enviou;
- Com relação aos *links* enviados por *e-mail*, na dúvida, não clique no mesmo;
- Não acessar conta bancária por meio de *links* contidos em *e-mails*;

7.1 DISPOSITIVO DE SEGURANÇA

Caso receba alguma mensagem ou ligação de terceiros. Nunca forneça o número do seu dispositivo eletrônico (senha, código, conta, *token* e etc).

Recomendamos algumas boas práticas – proteja seu celular:

- Em caso de perda ou roubo de celular, no qual o seu *token* esteja instalado, informe rapidamente a gerencia de atendimento da sua conta para que sejam seguidos os procedimentos adequados e o bloqueio imediato da conta, token.
- Sempre bom ter e manter atualizado um antivírus em seu dispositivo com acesso as suas transações financeiras, o vírus também pode invadir seu celular. Por isso, mantenha seu aparelho atualizado para garantir a segurança de suas informações. Outras ferramentas de controle de segurança, como um *firewall*, anti-spam (para filtrar mensagens não solicitadas) são bem-vindas.
- Evite deixá-lo exposto para impedir o acesso às suas informações. Não confie seu dispositivo móvel para acesso de terceiros, não é uma boa ideia, seus dados mesmo protegidos por senha, podem ficar armazenados e facilitar o acesso indevido.

8. BACKUP DOS SEUS DADOS

Faça *backups* regularmente de seus dados críticos, e teste se eles podem ser restaurados de forma íntegra. Isso reduzirá o risco de quaisquer dados contra roubo, danos físicos, incêndios ou até mesmo *ransomware*. Adicionalmente, você não pode ser chantageado por ataques de *ransomware* com seu *backup* em dia e facilmente recuperável.

Utilize ferramentas que automatizem o *backup* não apenas para economizar tempo, mas também que garanta a versão mais recente de seus arquivos. Lembre-se ao fazer o *backup*, verifique o tamanho e o tempo para recuperação dos dados que precisará acessar após qualquer incidente.

8.1 QUAIS DADOS FAZER BACKUP

Identifique o que precisa ser copiado, incluindo arquivos, *e-mails*, contatos salvos no seu dispositivo. Faça *backup* do seu negócio todos os dias, isso pode salvar informações uteis e importantes;

8.2 MANTENHA SEU BACKUP SEPARADO DA ORIGEM

Seja em um dispositivo USB (*pendrive*), em uma unidade apartada ou em um computador separado, o acesso aos *backups* de dados deve ser restrito e seguir as recomendações abaixo:

- Certifique-se de que o dispositivo que contém o *backup* não esteja permanentemente conectado ao dispositivo que contém a cópia original e que os dados sejam restritos, com acesso somente do responsável.;
- Armazene em um local separado da origem.

A SEGURANÇA TAMBÉM DEPENDE DE VOCÊ!