CODERN

AUTORIDADE PORTUÁRIA

Dicas de Segurança da Informação para nosso dia a dia

OBJETIVO

O material que chega até você tem o objetivo de dar dicas sobre como manter suas informações – pessoais, profissionais e comerciais – preservadas.

SEGURANÇA DA INFORMAÇÃO, O QUE É?

São procedimentos de proteção para resguardar o valor das informações de uma determinada pessoa ou empresa de ameaças como fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e desastres naturais.

POR QUE DEVO ME PREOCUPAR?

As ferramentas de segurança da informação são uma forma eficaz de reduzir os riscos de uso indevido de seus dados, tais como:

- Utilização de senhas e números de cartões de crédito furtados;
- Acesso não autorizado à conta de internet;
- Visualização, alteração ou destruição de dados pessoais por terceiros;
- Roubo de identidade nas redes sociais;
- Corrupção do sistema operacional do computador;
- Envio de e-mail por terceiros;
- Invasão de computadores e disseminação de vírus.

PRINCÍPIOS BÁSICOS

A segurança da informação é baseada em quatro conceitos fundamentais:

CONFIDENCIALIDADE

Prevê que as informações relacionadas a uma determinada pessoa NÃO devem ser reveladas a ninguém que não esteja autorizado a vê-las. O acesso não autorizado ao seu computador e aos dados nele contidos é um exemplo de quebra da confidencialidade.

INTEGRIDADE

Garante que a informação mantenha todas as características originais estabelecidas pelo proprietário da informação.

Portanto, se alguém alterar alguma informação contida em seu computador sem autorização estará infringindo a integridade dela.

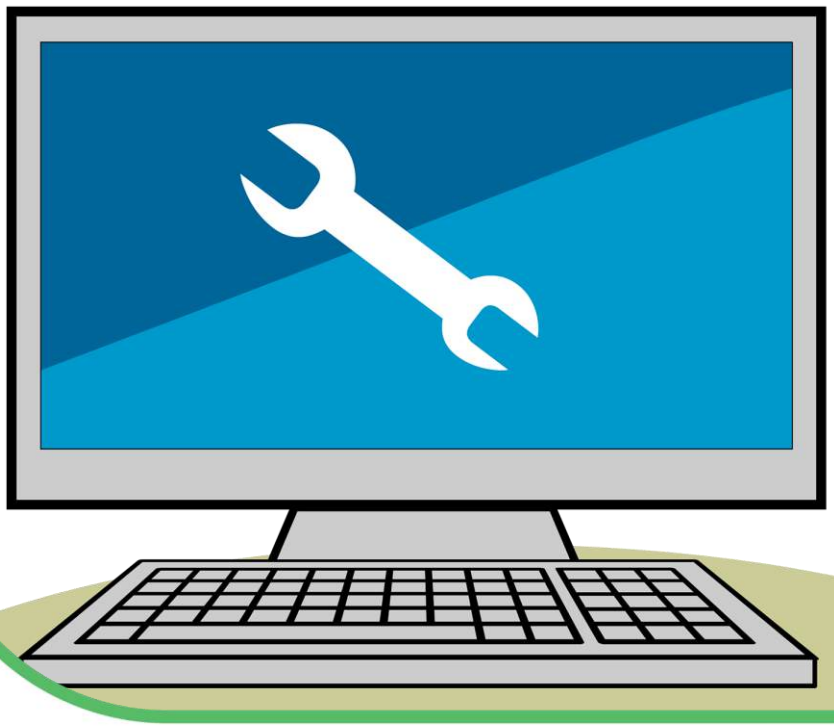
DISPONIBILIDADE

Avaliza que a informação esteja disponível para o uso legítimo, ou seja, por aqueles usuários autorizados por seu proprietário.

AUTENTICIDADE

Ratifica que a informação é proveniente das fontes anunciadas, ou seja, evita que outros usuários acessem a sua caixa de e-mail e enviem mensagens em seu nome, por exemplo.

PRINCIPAIS SISTEMAS DE SEGURANÇA DA INFORMAÇÃO



Para garantir os princípios básicos da segurança da informação existem ferramentas e ações que minimizam as ameaças mais frequentes. Conheça alguns desses sistemas:

- **Firewall:** dispositivo que aplica regras de segurança para controlar o fluxo de entrada e saída de informações na rede.
- **Antispam:** ferramenta que analisa os e-mails recebidos, identificando possíveis ameaças.
- **Antivírus:** programas instalados no computador que detectam, anulam e removem os vírus e outras ameaças.

CONFIGURAÇÕES:

Para que os computadores não sejam alvo de instalações indesejadas são necessárias algumas medidas de configuração de segurança para que as vulnerabilidades sejam diminuídas. São elas:

- Apenas contas como perfil de administrador do sistema em seu computador pessoal podem realizar todas as configurações e instalações. As demais contas que serão usadas não devem ter direitos de instalação ou configurações avançadas. A medida impede que aplicativos maliciosos tenham permissão para se instalar em seu computador.
- Habilite o Firewall em seu sistema operacional.
- Habilite a opção de bloquear pop-ups(janelas indesejáveis) de seu navegador.
- Desabilite a opção de execução automática de aplicativos em seu navegador.
- Configure seu antivírus para que faça a atualização toda vez que você entrar no computador.

AMEAÇAS À SEGURANÇA DA INFORMAÇÃO

ENGENHARIA SOCIAL E PHISHING

Por meio de persuasão, o impostor se utiliza da confiança das pessoas para obter informações que podem ser utilizadas para ter acesso não autorizado a dados importantes ou sigilosos.

Esse método de ataque pode ser executado por sites ou e-mail (Phishing), telefone ou presencialmente (Engenharia Social). O sucesso dessa ação depende única e exclusivamente da decisão das pessoas em fornecer as informações.

Existem algumas formas de dirimir esse tipo de ameaça:

- Nunca passe informações pessoais e corporativas a pessoas desconhecidas.
- Guarde documentos sigilosos em lugarseguro.
- Inutilize documentos antes de descartá-los.
- Bloqueie seu computador ao se ausentar.

CÓDIGOS MALICIOSOS (MALWARES)

Termo genérico que abrange todos os tipos de programas especificamente desenvolvidos para executar ações maliciosas em um computador. Geralmente, infectam o sistema operacional e são utilizados para obter senhas e dados confidenciais do usuá- rio ou utilizam a máquina para se espalhar a outros computadores.

Exemplos de Malwares: vírus, cavalo de Tróia, keyloggers (memorizadores de teclas) e spyware (programa espião).

Que cuidados devem ser tomados contra os malwares?

- Não abra anexos com extensões de arquivos duvidosos como .exe, .bat, .com, .vbs, .zlo, .htm, .html.
- Não abra e-mails de pessoas desconhecidas.
- Não cadastre seu e-mail em sites não confiáveis.
- Não entre em páginas de conteúdos duvidosos.
- Ao entrar em páginas de transações financeiras (bancos, compras e outros) verifique a integridade do site.

- Tenha um antivírus instalado no computador e o mantenha sempre atualizado. Faça varredurasfrequentemente.
- Mantenha seu Sistema Operacional sempreatualizado.
- Não instale softwares que não sejam licenciados.
- Antes de utilizar CDs, DVDs, pendrives e HDs externos sempre faça a varredura de antivírus.

SENHAS

LEMBRE-SE:

Sua senha é pessoal e intransferível!

PREVINA-SE:

- Ao digitar a sua senha, certifique-se de não estar sendo observado.
- Só forneça sua senha para outras pessoas em caso de extrema necessidade e depois a altere o mais rápido possível.
- Não utilize computadores públicos, como o de Lan houses, cybercafés e estandes de eventos para realizar operações com senhas.
- Troque frequentemente a sua senha.

Seja na internet ou em qualquer outro sistema relacionado a computadores, a senha representa uma assinatura, uma autenticação utilizada no processo de verificação de identidade do usuário que comprova que ele é realmente quem diz ser.

COMO ELABORAR UMA BOA SENHA?

Uma boa senha é aquela que o usuário se lembra facilmente, mas é difícil para qualquer outra pessoa adivinhar. A combinação deve ter, pelo menos, oito caracteres entre letras maiúsculas e minúsculas, números, espaços e símbolos (fique ligado nos comunicados sobre o tema e pegue todas as dicas necessárias).

Descarte opções óbvias como nomes, sobrenomes, números de documentos, placas de carros, números de telefones e datas. Esses dados podem ser obtidos e uma pessoa mal intencionada utilizálos para tentar se autenticar como você. Números e letras sequenciais também estão entre opções de tentativa de um impostor.

Alguns métodos como substituir letras por números (a letra i pelo número 1, a letra O pelo zero ou o A pelo 4) ou trocar as letras de um nome por suas anteriores no alfabeto também podem fortalecer a senha. Se você precisar anotá-la, não a identifique como uma senha e guarde-a em um lugar seguro.

De posse da sua senha, qualquer um pode ler e enviar e-mails em seu nome, acessar documentos, contas bancárias e seu perfil nas redes sociais, obter informações dos dados armazenados em seu computador e se esconder atrás da sua identidade para realizar ataques contra computadores de terceiros.

NAVEGAÇÃO SEGURA NA INTERNET

ATENÇÃO:

Se o cadeado estiver aberto, a conexão não é segura.

Para garantir a sua privacidade e a segurança do seu computador, existem cuidados que devem ser tomados ao acessar páginas na internet. Com esses procedimentos você pode evitar riscos como a instalação indesejada de programas maliciosos, acessos a sites falsos de instituições bancárias ou de comércio eletrônico e envio involuntário de informações confidenciais.

MEDIDAS PREVENTIVAS

- Mantenha seu navegador de internet sempre atualizado.
- Somente acesse páginas de instituições financeiras e de comércio eletrônico digitando o endereço diretamente no navegador.
- Certifique-se da procedência do site e da utilização de conexões seguras ao realizar transações via web.
- Não clique em links de páginas não confiáveis.

COMO IDENTIFICAR UMA CONEXÃO SEGURA

Existem pelo menos dois itens que podem ser visualizados na janela do navegador que demonstram a segurança das informações transmitidas pelo site visitado. O primeiro é o endereço eletrônico que deve começar com https://; o s indica que o endereço em questão é seguro.

O segundo item, normalmente, é um “cadeado fechado” apresentado na barra de endereço sou na barrade status na parte inferior da janela do browser. Esse símbolo representa que a página foi validada como autêntica por uma entidade certificadora.

CRIPTOGRAFIA E CERTIFICADO DIGITAIS

A criptografia tem como objetivo garantir a confidencialidade dos dados, transformando uma mensagem ou conexão original em outra ilegível, de forma a ser conhecida somente por seu destinatário, o que a torna difícil de ser lida por alguém não autorizado.

O uso dessa técnica trouxe bastante segurança para a navegação na internet. Um dos maiores benefícios são as transações bancárias (internet banking) e compras com cartões de crédito em sites de comércio eletrônico.

Já os certificados digitais têm a função de garantir a autenticidade dos sites, certificando que o endereço acessado é autentico e que a transação está sendo realmente criptografada.

CUIDADOS BÁSICOS COM AS REDES SOCIAIS

As mídias sociais são ferramentas que permitem a interação entre pessoas. Apesar de positivo, o grande crescimento do uso – pessoal ou comercial – desse tipo de canal de comunicação traz com ele alguns riscos que devem ser avaliados.

IDENTIFICANDO AS AMEAÇAS

- **Furto de identidade:** impostores que usam as informações postadas nas redes sociais para criar contas de e-mail, emitir documentos e criar perfis para se passar pelo usuário.
- **Phishing:** pessoas que se passam por empregados de uma empresa confiável para obter informações. Geralmente utilizam propagandas chamativas, para que o usuário sinta-se atraído e preencha formulários ou envie informações pessoais.
- **Danos à imagem e a reputação:** além de tomar cuidado para não denegrir a própria imagem com as informações postadas, o usuário deve se proteger de pessoas que podem apropriar-se delas para fazer difamação, injúria e calúnia.
- **Vazamento de informações:** as informações são valiosas para as pessoas e empresas. Uma vez vazadas nas redes sociais, podem gerar grandes prejuízos financeiros e de imagem.
- **Sequestros:** as informações publicadas pelo usuário nas redes sociais – como locais que costumam frequentar, fotos de familiares e pertences – podem ser úteis aos criminosos para escolher suas vítimas de sequestros ou roubos.

PRECAUÇÕES

- Ao entrar nasredessociais, leia o termo de uso e procure pelas configurações de privacidade, restringindo o acesso somente para amigos.
- Troque a senha frequentemente. Assim, você diminui o risco de pessoas não autorizadas acessarem sua conta.
- Nunca publique informações pessoais como endereços de e-mail e residencial, número de telefones, de identificação ou de cartões de crédito.
- Seja seletivo para aceitar amigos. Não aceite convites de amizades de pessoas desconhecidas.

- Monitore constantemente a sua rede social para identificar possíveis mensagens enviadas em seu nome.
- Tenha cuidado com compartilhamento de informações pessoais e fotos, pois elas podem ser replicadas por seus amigos.
- Evite a utilização de funções de localização “check-in” de forma pública.
- Cuidado ao clicar em links, mesmo os enviados por amigos. Eles podem ter tido a máquina invadida ou o perfil clonado.
- Caso utilize aplicativos de redes sociais em seu tablet ou smartphone, configure uma senha para bloquear o aparelho.
- Converse com seus filhos e/ou netos sobre os riscos e ameaças das redes sociais e os orientem sobre as regras básicas de segurança e privacidade.

OS 10 MANDAMENTOS DA SEGURANÇA DA INFORMA ÇÃO

1. Utilize senhas difíceis de serem descobertas;
2. Altere sua senha periodicamente;
3. Tome cuidado com downloads;
4. Tome cuidado com e-mails de remetentes desconhecidos;
5. Evite sites com conteúdo duvidosos;
6. Não abra anexos de e-mails desconhecidos;
7. Tome cuidado com compras na internet;
8. Tome cuidado ao acessar sites de bancos;
9. Não revele informações sobre você na internet;
10. Ao informar dados em sites, verifique se a página é segura (com prefixo“https”).

A Segurança da Informação é uma preocupação de todos!

www.codern.com.br