Cartilha Introdução à Segurança Digital

COGEL
Companhia de Governança Eletrônica de Salvador

Secretaria de Inovação e Tecnologia

SALVADOR
PREFEITURA

O que é Segurança Digital, e por que é importante para você?

A Segurança Digital se refere às práticas e medidas utilizadas para proteger dispositivos, dados, informações e atividades realizadas no ambiente digital.

Com o aumento do uso da internet e tecnologias digitais em nosso cotidiano, Segurança Digital tornou-se crucial para garantir a privacidade, proteger contra ameaças cibernéticas e evitar prejuízos financeiros e pessoais.

Resumindo:

Segurança Digital é como um escudo que protege suas informações na internet.

É importante porque todos nós queremos manter nossos dados pessoais, fotos, dados bancários e e-mails em segredo, longe dos olhos dos curiosos, certo?

Noções Básicas de Ameaças Online

Existem algumas ameaças na internet, que são como vilões, tentando roubar suas informações.

Vamos conhecer algumas delas. Apresentamos as principais ameaças online e como elas podem afetar você:

Malware:

São programas ruins que podem prejudicar seu computador ou celular, corrompendo arquivos e/ou roubando suas senhas.

Malware

Malware é um termo genérico usado para descrever programas maliciosos que são projetados para danificar, acessar informações ou obter controle não autorizado sobre sistemas e dispositivos. Alguns tipos comuns de Malware, são:

Vírus: Programas que se anexam a arquivos legítimos e se replicam quando esses arquivos são executados, prejudicando o sistema. Quando você executa um arquivo infectado, ele danifica seu seus Windows, apagando arquivos, deixando a máquina lenta ou até mesmo danificando placa-mãe ou disco rígido de seu equipamento.

Trojan (Cavalo de Troia):

São programas que trazem dentro de si códigos maliciosos para enganar os usuários e realizar ações sem o o seu conhecimento. Tanto podem danificar como celular, tablet, SmatTVs, laptops e outros, como podem roubar dados bancários eu só enviando pela rede para a pessoa que o desenvolveu.

Spyware:

Programas que monitoram atividades do usuário sem consentimento, espionando e roubando informações pessoais e confidenciais da vítima.

Ransomware:

Malware que bloqueia o acesso aos arquivos ou sistema do usuário e exige um resgate (pagamento) para libera-lo. Uma vez infectada, a vítima fica sem acessar os dados HD, SSD, pendrive e afins. Estes dispositivos ficam criptografados.

Imagine que você foi de bicicleta na praia, deixou ela na areia foi tomar banho de mar, Nesse intervalo, alguém se aproxima e coloca um cadeado com um bilhete: "Faça o pix que tiro a corrente e o cadeado de sua bike", O Ransomware vai fazer isso com seu dispositivo, só que ao invés de pix, o pagamento é em criptomoedas, pada dificultar o rastreamento.

Phishing:

É como um truque em que vilões fingem serem outras pessoas para te enganar. Eles enviam mensagens falsas pedindo suas senhas ou informações pessoais. Esta técnica de engenharia social é utilizada por cibercriminosos, que se passam por instituições e entidades confiáveis para obter informações sensíveis e confidenciais, como senhas, números de cartões de crédito ou informações bancárias.

. Geralmente, isso é feito através de e-mails, mensagens ou sites falsos que imitam instituições legítimas. Por isso NUNCA forneça seus dados por telefone ou preencha formulários desconhecidos, enviados por e-mail, mensageiros ou qualquer outro meio.

Ataques de Força Bruta:

Apesar do nome, aqui os vilões não batem em ninguém para conseguir suas senhas. Eles tentam adivinhá-las utilizando programas específicos. Neste tipo de ataque, os ladrões experimentam várias combinações de senhas até encontrar a correta para acessar uma conta ou sistema. O programa utilizado usa inúmeras possibilidades até conseguir o acesso às suas informações.

Vazamento de Dados:

É quando informações pessoais são expostas sem permissão, podendo ser usadas de maneira errada. A exposição não autorizada de dados pessoais e financeiras ou senhas são realizada por criminosos que exploraram falhas de sistemas como redes sociais, servidores de e-mail, instituições financeiras (públicas ou privadas), entre outros que possuam base de dados de clientes.

Wi-Fi Público Inseguro:

Redes Wi-Fi grátis, em lugares públicos, são perigosas e não devem ser acessadas. Pessoas mal intencionadas poderão monitorar seu acesso à internet e roubar suas informações.

Por isso é desaconselhável o acesso dessas redes, pois elas possuem o mínimo de segurança possível em sua configuração podem apontar para servidores falsos, que roubarão seus dados.

DICAS PARA PROTEGER SUA SEGURANÇA DIGITAL

Aqui estão algumas dicas simples para manter suas informações seguras na internet:

Mantenha tudo atualizado:

Sempre atualize seu celular, computador e programas. Utilize um bom antivírus e firewall pessoal, evite usar programas piratas, use somente os originais. Se não pode comprar, use uma versão similar open source (código aberto) ou se inscreva em algum programa de aquisição de programas educacionais.

O que você prefere pagar por um programa, ou ter suas contas e dados bancários roubados?

Fica a dica!!!!!

Crie senhas fortes:

Use senhas difíceis com letras, números e símbolos misturados. Evite usar a mesma senha para várias contas. Não anotes senhas em blocos de notas, papeis avulsos na carteira, não salve em e-mails ou mensageiros, use sempre senhas longas, não use datas comemorativas ou de significado comum.

Links e Anexos:

Não clique em links ou abra arquivos que você não conhece, tanto por e-mail ou mensageiros, entre sempre em contato com a pessoa que te mandou o link e valide o envio.

NÃO CLIQUE EM LINKS DE PROPAGANDAS DESCONHECIDAS, JOGOS, CASAS DE APOSTAS OU PRODUTOS MILAGROSOS OU BARATOS DEMAIS.

Autenticação 2FA:

Ative a autenticação de dois fatores (2FA) sempre que possível. Ela é utilizada da seguinte forma: você insere sua senha na aplicação e a mesma solicita uma confirmação em seu celular via SMS ou pede para que você gere um código em algum autenticador instalado em seu celular. Um bom número de sistemas esta ultilizando essa forma de autenticação.

Agora cuidado com sites que pedem para usar e-mails do Google, Microsoft, ou Facebook. Não use em sites desconhecidos, principalmente se terminarem o endereço com ru, ex: http://abc.ru.

A autenticação em dois fatores adiciona uma camadaextra de proteção às suas contas.

Faça backups:

Guarde cópias de seus arquivos importantes em um lugar seguro. Use vários pendrives, discos SSD, de preferência de marcas conhecidas e confiáveis, contrate serviços confiáveis de armazenamento na internet.

Ambiente Corporativo:

No ambiente corporativo, os cuidados com a segurança são redobrados e todo usuário deve contribuir, observando as orientações abaixo:

Antes de utilizar dispositivos pessoais de armazenamento, peça para o NTI passar o antivírus;

Evite o uso de e-mails pessoais durante a jornada de trabalho, essas plataformas não possuem as mesmas políticas de segurança usadas em sua corporação, criando assim uma brecha na segurança;

No seu acesso a internet, sempre que tiver alguma dúvida durante a navegação solicite suporte do NTI;

Use seu e-mail corporativo para assuntos relacionados ao trabalho, é seguro pra você e para quem estiver se comunicando contigo, nossas politicas de segurança, garantirão a segurança da informação.

Ambiente Corporativo:

Além dos cuidados tecnológicos, precisamos ficar atentos a um fator muito importante para segurança corporativa, o cuidado com ataques engenharia social, mas o que é isso? São ataques que visam enganar suas vítimas, tentando utilizar informações falsas como verídicas, fique atento as dicas:

Valide os contatos telefônicos, sempre pedindo informações completas que possam identificar o contato, retorne contato com a empresa validando essas informações;

Destrua todas informações que não serão mais utilizadas, tanto digitalmente, e principalmente as informações físicas, o lixo é uma fonte preciosa para consulta em um ataque digital;

Tenha cuidado ao transmitir informações sensíveis, nunca as faça por telefone ou mensageiros ou celular, certifique-se de usar solução segura da empresa.

Quando tratar de assunto sensível, garanta que somente as pessoas envolvidas estejam presentes, para evitar vazamento das informações.

Lembre-se, a Segurança Digital é como um escudo que você usa para se proteger dos vilões da internet. Seguindo essas dicas, você estará mais seguro enquanto navega e aproveita tudo que a internet tem para oferecer!

Não esqueça segurança digital é uma responsabilidade contínua. Adotar práticas seguras e estar sempre alerta ajuda a proteger seus dados e sua privacidade em um mundo cada vez mais conectado.

COGEL
Companhia de Governança Eletrônica de Salvador

Secretaria de Inovação e Tecnologia

SALVADOR
PREFEITURA