INFORMATIVO: ATAQUES CIBERNÉTICOS E COMO SE PREVENIR

A ocorrência de ataques cibernéticos no Brasil e no mundo está cada vez mais frequente. Usuários têm suas informações pessoais divulgadas, Órgãos do Governo que ficam fora do ar, empresas vítimas de extorsão e provedores alvos de ataques hackers. Veremos no presente informativo algumas informações importante sobre este assunto.

O QUE SÃO ATAQUES CIBERNÉTICOS ?

São atentados que objetivam danificar, destruir ou obter informações alheias e geralmente ocorrem quando há falhas de segurança na rede ou sistema.

Abaixo, citaremos 3 tipos de ataques mais comuns:

-> Ransomware: trata-se de software malicioso que infecta um computador/rede e bloqueia o acesso ao sistema de dados. Muitas vezes, os criminosos solicitam dinheiro para a liberação dos respectivos dados.

-> Phishing: são criados gatilhos que direciona o usuário para um site falso ou que não possui segurança para roubar dados importantes como senhas, número de cartões, CPF...

-> Spoofing: visa falsificar a identidade de uma pessoa ou empresa, para enganar os outros por meio de sistemas para obter informações. Por exemplo: o atacante envia e-mails parecendo ser de remententes conhecidos e confiáveis para coletar dados pessoais, solicitar dinheiro...

Como o usuário pode se prevenir?

- atualize sempre o seu sistema operacional;
- instale software antivírus;
- deixe seu smartphone sempre protegido e use PIN sempre que possível;
- cuidado com os aplicativos que baixar e suas permissões;
- ative a autenticação de dois fatores;

- tome muito cuidado onde você clica, os hackers costumam enviar e-mails e mensagens falsas com link de acesso para roubar os seus dados.

Como a Prestadora está se prevenindo?

Considerando que a segurança da informação deve ser tratada como assunto primordial e os ataques estão cada vez mais frequente, a Prestadora, afim de prezar pela segurança de sua empresa e seus usuários, conta com a presença de especialistas para realizar tarefas de prevenção, monitoramento, mapeamento de vulnerabilidades e acompanhamento de possíveis incidentes.

Caso haja dúvidas sobre o tema, estamos à disposição para auxiliá-los.

SEGURANÇA: PRINCIPAIS ASPECTOS DA AUTENTICAÇÃO DE DOIS FATORES

O QUE É ?

Também conhecido como "aprovação de login", "two- factor authentication" e "verificação em dois passos", se refere à um recurso que acrescenta uma segunda camada de segurança no processo de login. Assim, o segundo fator pode ser por exemplo o o envio de um código de verificação por meio de um SMS com o referido código, ou até mesmo um link no e-mail para acesso.

POR QUE UTILIZAR A VERIFICAÇÃO EM DUAS ETAPAS?

Infelizmente, usar somente as senhas pode não ser suficiente para que as contas na internet sejam protegidas, pois, muitas vezes são de fácil descoberta através de técnicas de engenharia social.

Neste sentido, caso a pessoa utilize a verificação em dois fatores, certamente, a sua conta será dificilmente invadida, pois, a conta somente será invadida se houver com sucesso a realização dos dois passos de segurança.

Dicas do que usar para o 2º passo:

- Use senhas de difícil adivinhação, algo que SOMENTE você saiba;
- Escolha uma pergunta de segurança;
- Faça referência a algo que apenas você possua;
- Faça referência a algo que apenas você possua, evitando nomes ou dados pessoais de fácil adivinhação;
- Sempre que possível, utilize impressão digital, rosto, olhos ou até mesmo a voz;

Alguns exemplos de serviços que podemos fazer a autenticação em dois fatores:

- Redes Sociais;
- Internet Banking;
- Armazenamento em núvem;
- Aplicativo de WhatsApp;

QUAIS CUIDADOS DEVEMOS TER?

- Mantenha o contato telefônico sempre atualizado, bem como um segundo contato alternativo;
- Cuidado para não perder o celular, e se certifique que a posse está de fato com você, isto é muito importante quando configurado o 2º passo por meio de SMS;
- Prefira aplicativos que não utilize internet;
- Preste muita atenção nas criações das senhas, evite nomes pessoais, datas, ou demais informações de fácil descoberta ou disponibilidade;
- Instale aplicativo antivírus;
- Sempre verifique se está usando conexão segura, e preste muita atenção ao clicar em links desconhecidos;
- Proteja sempre seus dados e seu computador.

RECOMENDAÇÕES DE SEGURANÇA AOS USUÁRIOS

A disseminação de informação é indispensável para que haja um ambiente online cada vez mais seguro e confiável. Neste sentido, é notório também que, os clientes e usuários possuem inteira responsabilidade pelos atos que executam com seu IP.

Diante disso, a equipe FASTNET preparou uma cartilha com algumas recomendações e cuidados a serem tomados por cada um dos usuários, afim de disseminar dicas relevantes quanto à Segurança de informações.

Assim, considerando que, cada vez mais se ouve falar de clonagens de aplicativos, cartões e invasões, segue abaixo algumas dicas de **COMO SE PREVENIR:**

- Recomendamos manter suas senhas em completo sigilo, não anotar e sim memorizá-las, alterar sempre que se sentir inseguro, além de criar senhas de difícil adivinhação.
- Faça, sempre que possível, o backup para evitar a perda de informações e dados em caso de mau funcionamento.
- Desconfie sempre de contatos telefônicos que solicitem dados, pois, há muita fraude em ligações falsas, nas quais são solicitadas informações pessoais para a realização de fraudes.
- Se atentem aos e-mails recebidos e não solicitados, estes são chamados de SPAM, eles são enviados em massa e possuem a finalidade de publicidade e disseminação de informações falsas ou ilegais.
- Cuidado com o recebimento de e-mails ou mensagens aparentemente reais, que objetivam obter suas informações pessoais, como por exemplo número de RG, CPF e dados bancários, para posteriormente cometer fraudes eletrônicas. Essa prática é chamada de Phishing.
- Utilize a autenticação em duas etapas, ela adiciona uma segunda camada de proteção no acesso a uma conta. É um recurso opcional em diversos aplicativos, como por exemplo: e-mail, WhatsApp, redes sociais, internet banking, etc...

- Desconfie de links ou pedidos de pagamentos recebidos via mensagens eletrônicas, mesmo que vindos de pessoas conhecidas.
- Caso queira, reduza a quantidade de informações sobre você na internet;

LEMBRE-SE : Sempre usem conexões seguras, seja seletivo com aplicativos, observem sempre as configurações de privacidades, limitem a coleta de dados por cookies e limpe frequentemente o histórico de navegação.

Conte conosco para sanar quaisquer dúvidas pelos seguintes canais de atendimento: (79) 3045-4880 ou 0800 079 2399

Equipe Fastnet.