

Conselhos

✓ Malware

Os códigos maliciosos são uma das principais ameaças virtuais. Denomina-se malware qualquer aplicação (software) que possui finalidade prejudicial. Existe uma grande quantidade destas ameaças: vírus, spyware, adware, worms, trojans, rootkits, etc. Todas elas com diversas ações sobre o Sistema. Para a devida proteção, os usuários devem contar com uma ferramenta antivírus que possua capacidade de detecção pró-ativa. Além disso, é recomendado cuidado ao navegar pela Internet, não baixar arquivos desconhecidos e manter tanto as aplicações como o Sistema operacional sempre atualizados.

✓ E-mails

As principais ameaças que se propagam pelos e-mails são os Spams (utilizados com fins publicitários e de propagação de malware), o Phishing (utilizado para roubar informações pessoais) e o SCAM (com intuito de roubar dados financeiros). Entre as melhores práticas para a prevenção, se incluem: não abrir e-mails desconhecidos e preferencialmente contar com uma ferramenta anti-spam para filtrá-los, verificar os arquivos anexos com antivírus antes de sua execução, não enviar e-mails em cadeia (e quando o fizer, utilizar a opção de cópia oculta) além de evitar publicar o endereço do e-mail.

✓ Navegação Web

A Internet é o principal foco de propagação de ameaças e vem se transformando nos últimos anos, pois um ataque pode ser executado diretamente pela web. O usuário deve fazer o uso consciente de seus recursos, evitando o acesso a websites que possam ser perigosos ou de reputação desconhecida, evitando baixar arquivos desconhecidos, minimizando as informações pessoais que são publicadas na internet, e evitando o acesso a portais que solicitem informações importantes, como acesso a websites de Bancos (instituições financeiras) em computadores públicos ou compartilhados, entre outros.

✓ Transações Online

A utilização de Bancos online e outros serviços de e-commerce vem crescendo nos últimos anos. Por tal motivo, os hackers criaram ataques para obter as credenciais de acesso a estes sistemas, e posteriormente roubar os recursos financeiros das vítimas. A recomendação inicial consiste em não utilizar estes serviços em computadores públicos ou compartilhados, mas fazê-los apenas a partir de um computador cuja segurança seja gerenciada pelo usuário. Além disso, este computador deve ter uma proteção antivírus instalada e o usuário deve verificar se a informação confidencial está inserida unicamente em websites oficiais das Instituições.

✓ Roubo de Identidade

O roubo de identidade é uma das ameaças mais perigosas para o usuário. Uma vítima deste ocorrido poderá sofrer prejuízos sociais e econômicos. Para evitar ser vítima, é necessário cuidar das informações pessoais que são publicadas na Internet. Qualquer conteúdo que seja carregado na web pode ser acessado por terceiros e utilizado para o roubo de identidade. Nunca deve ser compartilhada a informação pessoal ou confidencial.

✓ Redes Sociais e Mensagens Instantâneas

As redes sociais são ferramentas de comunicação que são utilizadas por hackers para propagar suas ameaças. Como medidas de prevenção destacam-se o não estabelecimento de contatos com pessoas desconhecidas, não publicar a privacidade do perfil e cuidado com os conteúdos que se executam nestas redes. Os softwares de mensagens instantâneas também podem ser utilizados para propagar ameaças, e boas práticas de prevenção para os usuários são: não abrir arquivos que provenham de contatos desconhecidos ou que não sejam analisados previamente por um antivírus, não abrir os links enviados e alterar periodicamente a senha acesso (também nas redes sociais).