Conceitos de Segurança da Informação (antivírus, golpes comuns, senhas).

Segurança da informação é a proteção de dados de propriedade das organizações contra ameaças diversas. Mas além das grandes organizações, é também necessário que todos os indivíduos que navegam na internet tenham cuidado com seus dados. A seguir são listadas algumas ameaças que podemos encontrar ao navegar pela rede:

- *Malware*: esse é um termo para descrever um software mal-intencionado ou um código malicioso, que viola a rede por meio de uma vulnerabilidade, podendo ser utilizado para obter informações secretamente, prejudicar componentes do sistema ou bloquear acessos a ele.
- *Phishing*: essa é a prática de enviar comunicações fraudulentas que parecem vir de uma fonte confiável, geralmente por e-mail. O objetivo é roubar dados confidenciais, como senhas, ou instalar um *malware* na máquina da vítima.
- Ataque *man-in-the-middle*: quando os invasores se inserem em uma transação entre duas partes.
- Inserção de *SQL*: quando um invasor insere um código mal-intencionado em um servidor que usa SQL, forçando o servidor a revelar informações que não seriam expostas normalmente.
- *Ransomware*: tipo de malware que torna inacessíveis os dados armazenados em um equipamento, exigindo um pagamento de resgate para estabelecer acesso.
- *Spyware*: malware que espiona seu equipamento para obter qualquer tipo de informação, como senhas e dados bancários.
- *Cavalo de Tróia*: tipo de malware que permite acesso remoto ao seu computador.
- *Keylogger*: *malware* que captura o que é digitado pelo usuário, em geral, vem combinado com outros *malwares*.
- *Worm*: traduzindo o nome desse *malware*, Verme explora falhas no sistema operacional e de maneira silenciosa infecta a máquina se espalhando por outros dispositivos.

Para evitar ser atingido por malwares e *ransomwares*, é preciso ter atenção aos downloads de softwares gratuitos, legítimos ou não, ao acesso de websites infectados, ao clicar em falsas mensagens de erro ou janelas de pop-up e ao abrir e-mails. Há muitas formas diferentes de um malware se espalhar, mas ainda sim é possível se proteger. O antivírus também deve conter *Firewall*, um dispositivo de segurança que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.

Além de tomar todos os cuidados com as ações listadas anteriormente, é necessário ter um bom antivírus em seu computador e sempre manter seu sistema operacional atualizado. Um antivírus pode verificar se há algum malware em itens de download antes de abri-lo. Ele também permite que você realize uma verificação de todo o seu computador à procura de malware. Recomenda-se que essas verificações sejam feitas regularmente para detectar a presença da ameaça o quanto antes e evitar que ela se espalhe.

Nos computadores da faculdade é utilizado o antivírus *Kaspersky*. Esse antivírus possui quatro opções principais em sua tela de início: Proteção, Verificação, Atualizações e Opções. Na aba de Proteção, existem opções específicas para configurar diversos módulos, sendo possível realizar escaneamentos e varreduras no sistema e inclusive programar tarefas e adicionar exceções. Na aba de atualizações há informações a respeito de novas versões do software e da atualização do banco de dados. Em opções, é possível mudar a aparência e perfis particulares.

Também podem ser tomados cuidados para não ser vítima de *pishing*. Esse tipo de ameaça acontece através do e-mail, com mensagens alarmantes do seu banco ou de qualquer outra empresa dizendo que sua conta pode ser fechada. Quase sempre essas mensagens são golpes de *pishing*. As mensagens desse tipo de golpe parecem ser de uma empresa legítima, mas seu objetivo é roubar informações pessoas do destinatário ou até receber uma transferência em dinheiro.

Uma dica para se prevenir contra o *pishing* é ter em mente que a faculdade não solicita informações pessoais ou detalhes de conta por e-mail. Se você recebeu um e-mail desse tipo, entre em contato com um funcionário do departamento de informática da FEF e confirme se há realmente algum

problema. Não abra anexos desses e-mails suspeitos e nem clique em links incorporados, pois estes podem estar carregados de malwares.

Essas dicas podem ser tomadas para evitar quase todas as ameaças online, mas nenhuma delas dispensa os cuidados com sua senha. É fundamental a utilização de senhas fortes e não as repetir em todas as plataformas, pois, uma vez descobertas, um agente mal-intencionado terá acesso a todos os sites em que ela foi cadastrada. Senhas seguras são formadas por um misto de letras minúsculas e maiúsculas, números e caracteres especiais, e quanto mais longas, mais difíceis são de ser decifradas, são recomendados pelo menos 8 caracteres, com 14 sua senha será considerada muito segura. Na tabela abaixo é apresentado o tempo que um hacker precisará para quebrar sua senha em tentativas de força bruta, instantaneamente:

Número de caracteres	Apenas números	Letras minúsculas	Letras minúsculas e maiúsculas	Números, letras minúsculas e maiúsculas	Números, letras minúsculas, maiúsculas e símbolos
4	instantaneamente	instantaneamente	instantaneamente	instantaneamente	instantaneamente
5	instantaneamente	instantaneamente	instantaneamente	instantaneamente	instantaneamente
6	instantaneamente	instantaneamente	instantaneamente	1 segundo	5 segundos
7	instantaneamente	instantaneamente	25 segundos	1 minuto	6 minutos
8	instantaneamente	5 segundos	22 minutos	1 hora	8 horas
9	instantaneamente	2 minutos	19 horas	3 dias	3 semanas
10	instantaneamente	58 minutos	1 mês	7 meses	5 anos
11	2 segundos	1 dia	5 anos	41 anos	400 anos
12	25 segundos	3 semanas	300 anos	2k anos	34k anos
13	4 minuutos	1 ano	16k anos	100k anos	2m anos
14	41 minutos	51 anos	800k anos	9m anos	200m anos

Fonte: HowSecureismyPassword.net

Além dessas informações, é importante que, quando navegando na rede em computadores que não pertencem ao usuário, não permita que sua senha seja gravada em sites e sempre se lembre de sair das suas contas. Caso isso não seja feito, suas informações estarão em ameaça, visto que a próxima pessoa a acessar o computador terá acesso à sua conta e poderá cometer atos mal-intencionados.

Links para saber mais:

https://www.cisco.com/c/pt_br/products/security/what-is-network-security.html#~tipos – O que é segurança na rede

https://blog.intnet.com.br/tipos-de-virus-quais-sao-as-maiores-fontes-e-como-evitar/ - Maiores fontes de vírus e como evitar

https://cartilha.cert.br/malware/ - Tipos de malware

https://www.avg.com/pt/signal/how-to-create-a-strong-password-that-you-wont-forget - Como criar senhas seguras e fáceis de lembrar