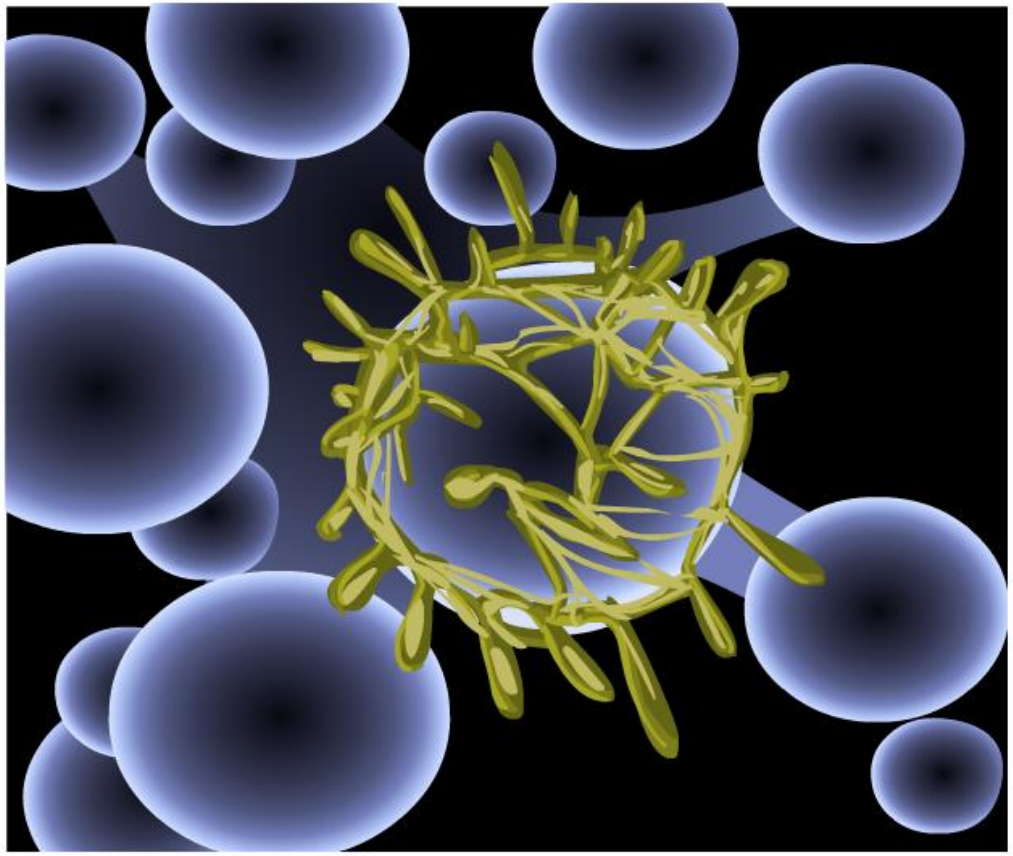
Módulo III – Aula 2
Hacker, Vírus, Senhas e Backups

Vivemos em uma sociedade que se baseia em informações e que exibe uma crescente propensão para coletá-las e armazená-las. Por isso a necessidade de se ter mecanismos de segurança realmente eficientes.

Nessa aula você estudará assuntos como *hacker,* vírus, dicas de como criar uma senha segura e outras maneiras de proteção.

Bons estudos!



Hacker

O *hacker* é uma pessoa que possui grande facilidade de análise, assimilação, compreensão e uma capacidade surpreendente de conseguir fazer o que quer (literalmente) com um computador. Ele sabe perfeitamente que nenhum sistema é completamente livre de falhas e procura por elas, utilizando técnicas variadas (aliás, quanto mais variado, mais valioso o conhecimento do *hacker*).

Os *hackers* utilizam vários métodos para quebrar senhas, como introduzir Cavalos de Tróia, farejar redes, quebra-cabeça, engenharia social e assim por diante.

Cavalo de Tróia

O nome é dado em homenagem ao presente dos gregos, que conseguiram penetrar na até então inexpugnável cidade de Tróia. Nesse caso, o *hacker* infiltra no alvo um programa semelhante a um vírus. Mas, em lugar de agir como tal, ele, na verdade, descobre senhas. Cada vez que o usuário escreve nome e senha, o Cavalo de Tróia grava os dados.

No momento programado para se conectar com seu criador, por meio do modem, ele transmite os dados que copiou.

Farejamento de redes

São programas criados por *hackers* que vasculham a circulação dos pacotes de dados transmitidos pela rede, buscando palavras como *password* e senha. Quando encontra essas palavras, o programa copia o pacote e o envia para o computador do *hacker*.

Os dados chegam codificados, mas geralmente os *hackers* conseguem descodificar as mensagens.

Engenharia social

Uma espécie de espionagem. Senhas com datas de nascimento, sobrenome ou nome dos filhos são muito comuns e se o *hacker* conhecer essas datas tentará usá-las.

Alguns chegam a arrumar emprego temporário na empresa que pretendem invadir e prestam atenção quando alguém digita senhas, afinal, é raro alguém esconder o teclado nessa hora! Pronto, a segurança foi embora.

Quebra-cabeça

Um jeito simples de desvendar senhas é a velha tentativa e erro. Funciona melhor com senhas de até seis caracteres, embora leve tempo. As tentativas não podem ser próximas umas das outras, ou há risco de levantar suspeitas. O *hacker* utiliza programas que montam todo tipo de combinação de letras e números.

"É um método muito difundido no Brasil, pois as senhas em geral são simples e os computadores desprotegidos."

(Fonte: www.futurodigital.cjb.net)

Outros apelidos dados a um *hacker*

Cracker

O *cracker* age como um *hacker*, com uma diferença: após fazer o serviço, precisa deixar um recado que passou por ali. Geralmente, são mensagens irônicas ou grosseiras. Sua ação é daninha e aniquiladora, destruindo partes do sistema ou até sua totalidade.

Também são atribuídos aos *crackers* programas que retiram travas em *softwares*, bem como os que alteram suas características, adicionando ou modificando opções, muitas vezes relacionadas à pirataria.

Phreaker

Um especialista em telefonia. Opera com ligações gratuitas (locais ou não), reprogramação de centrais telefônicas, instalação de escutas etc.

Esse profissional tem importância, pois ao detectar eventuais pontos críticos no sistema, permite protegê-lo de invasões.

Entretanto, pode tornar o sistema invisível em eventuais rastreamentos e até mesmo detectar ou forjar culpados para ligações fraudulentas.

Vírus e antivírus

O que é um vírus

Um vírus é apenas um programa que se autocópia e/ou faz alterações em outros arquivos e programas, de preferência sem o seu conhecimento e sem a sua autorização.

O nome é apenas uma analogia aos vírus biológicos, pelos danos que causam e pela forma como se propagam.

Os vírus não surgem do nada no computador. São criados por alguém e postos em circulação até que chegam em seu computador por meio de um programa, *e-mail*, pendrive ou página da Internet infectados.

Um vírus basicamente é um conjunto de instruções com dois objetivos: agregar-se a um arquivo para depois se disseminar sistematicamente para outros, sem a permissão ou comando do usuário. São, portanto, auto replicantes. Além disso, os vírus contêm instruções para agir conforme o seu criador deseja.

Podem se manifestar de diversas formas:

- ✓ mostram mensagens indesejadas.
- ✓ alteram arquivos.
- ✓ diminuem o desempenho do sistema.
- ✓ apagam arquivos.
- ✓ corrompem a tabela de alocação.
- ✓ apagam todo o disco rígido.

Classificação dos vírus

Benignos

Apenas exibem mensagens, muitas vezes em dias predeterminados, sem provocar danos maiores.

Malignos

Vírus que de fato afetam arquivos e programas, impedindo que o usuário execute determinadas operações. Muitas vezes, um vírus previamente concebido para ser benigno age destrutivamente por erro de programação do criador ou por *bugs*.

Macrovírus

São vírus que infectam arquivos de dados, como os do Word (.doc) e Excel (.xls). Não atacam arquivos executáveis (.exe). Esses vírus, geralmente, são multiplataforma, não importando o sistema operacional que atacam, seja Windows, Linux ou outros.

Programas antivírus

São programas para detectar vírus num computador, CDs, *pendrive*, MP3, MP4 e outros.

Quando um vírus é detectado, sua sequência de *bytes* é analisada. O programa antivírus, então, faz uma varredura no disco rígido sempre que o computador é ligado (ou quando antivírus é acionado), buscando uma sequência igual ou similar em seus arquivos. Encontrando essa sequência, acusa a infecção e, sempre que possível, faz automaticamente as correções necessárias.

Atualizar sempre

Embora os programas antivírus possuam catalogados, em seus bancos de dados milhares de vírus conhecidos, surgem a cada mês, em mídia, 100 novos.

Assim, é necessário atualizar constantemente o programa. Dependendo do programa, essa atualização é gratuita durante o primeiro ano após a compra e pode ser realizada diretamente pela Internet caso seu antivírus não seja totalmente *free* (gratuito).

Também é importante atualizá-lo sempre em à relação versão do *software*.

Sites de *download* de *software* como www.superdownloads.com.br, www.baixaki.com.br, www.gratis.com.br e outros estão sempre divulgando as versões mais recentes. Você também pode encontrar direto no *site* da empresa do antivírus.

Alguns programas antivírus

Tipo	Descrição
Virusscan	Produzido pela McAfee, um dos mais conhecidos no mundo. Disponível em versões para os vários sistemas operacionais, desde o Ms-DOs até o Windows.
Norton Antivírus - NAV	Produzido pela Symantec, o Norton Antivírus (também conhecido como NAV) encontra-se entre os mais populares hoje em dia.
Dr. Solomons Tool Kit	Possui aproximadamente 13 mil vírus listados, com uma interface bastante amigável.
AVG	Produzido pela Grisoft, possui uma versão gratuita. Um dos antivírus mais usados pelos usuários domésticos. Com um amplo banco de dados de vírus.
Panda	Desenvolvido pela Panda Security, foi desenvolvido especialmente para aquelas pessoas que não querem passar um bom tempo configurando todas as funções do antivírus, basta instalar e esqueça. Gratuito para testar por 30 dias.

Spyware* e *antispyware

Spyware é o termo usado para descrever *softwares* que executam determinados comportamentos, como publicidade, recolha de informações pessoais ou alteração da configuração do computador, normalmente sem o seu consentimento prévio. O *spyware* está muitas vezes associado a apresentações de publicidade (chamado *adware*) ou *software*s que detectam informações pessoais ou importantes.

Isso não significa que todo o *software* que fornece anúncios ou detecta as suas atividades *on-line* seja mau. Por exemplo, você pode assinar um serviço de música gratuito, mas "paga" pelo serviço aceitando receber anúncios publicitários de seu interesse. Se aceitar as condições e concordar com elas, pode considerar que se trata de um acordo justo.

Outros tipos de *spyware* fazem alterações no seu computador que podem ser aborrecedoras e provocar lentidão ou o bloqueio do computador. Esses programas podem alterar a página inicial ou página de pesquisa do seu *browser* da *web* ou adicionar componentes desnecessários ou indesejados ao seu *browser*. Esses programas também dificultam muito a reposição das configurações para a forma original (Fonte: www.microsoft.com).

Alguns programas de *antispyware*

Existem programas de antivírus que protegem de *spywares*.Esses programas também devem ser atualizados na sua lista de banco de dados, pois a cada dia surgem novos *spyware*. Veja os dois exemplos mais usados.

Tipo	Descrição
Spybot	Além de proteger contra *spyware*, pode remover rastros de uso, uma função interessante se você partilha o seu computador com outros usuários e não quer que eles vejam o que você está trabalhando. Desenvolvido por Patrick M. Kolla (www.safer-networking.org) e totalmente gratuito.
Ad-Aware	Produzido pela Lavasoft, um dos pioneiros no combate a *spywares*, prevenindo, detectando e removendo esses arquivos maliciosos, trazendo um computador livre dessas ameaças.

A senha perfeita

Será que existe a senha perfeita? Você estudou no inicio desta aula que *hackers* conseguem descobrir senhas de várias maneiras, então como criar uma senha difícil de quebrar, já que aparentemente o impossível está inalcançável? Aqui vão algumas dicas.

Aos administradores de rede

- ✓ Não use a conta do super usuário ou administrador para outros setores/ funcionários.
- ✓ Crie grupos por setores/áreas afins.
- ✓ Crie contas dos usuários de acordo com seus nomes, dentro dos grupos.
- ✓ Faça troca de senha periodicamente, o ideal que a cada três meses e no máximo seis meses.
- ✓ Faça a troca de senha sempre que houver suspeita de vazamento.
- ✓ A senha de cada usuário é pessoal e intransferível. Proíba rigorosamente que ela seja cedida para outra pessoa.

O responsável por cada setor (ou gerente geral) deverá ter as senhas dos seus funcionários, em local seguro, para casos de emergência.

Jamais escreva a senha num pedaço de papel e o cole no teclado ou monitor, nem o coloque na sua gaveta destrancada.

A senha perfeita

Ao usuário, não utilizar:

- ✘ mesmo nome do usuário (login);
- ✘ senha em branco;
- ✘ palavras óbvias, como “senha”, “pass” ou “password”;
- ✘ mesma senha para diversos usuários;
- ✘ primeiro e último nome do usuário;
- ✘ nome do marido, esposa, pais ou filhos;
- ✘ informações pessoais (placa do carro, data de nascimento, telefone, CPF);
- ✘ somente números;
- ✘ palavra contida em dicionário (tanto português quanto inglês);
- ✘ palavra com menos de 6 caracteres.

Utilize:

- 👍 letras minúsculas e maiúsculas
- 👍 palavras com caracteres não alfabéticos (números ou sinais);
- 👍 fácil de lembrar para não ter que escrever;
- 👍 fácil de digitar (sem ter que olhar o teclado).
- 👍 primeira ou segunda letra de cada palavra de um título ou frase fácil de memorizar;
- 👍 junção de duas palavras curtas com sinal de pontuação;
- 👍 junção de duas palavras pequenas de línguas diferentes.

Backup

Backup é uma cópia dos arquivos que julgamos mais importantes ou aqueles considerados fundamentais. Com o uso cada vez mais constante de computadores, um sistema de *backup* que garanta a segurança e disponibilidade em tempo integral de dados é indispensável.

Apesar de ser uma medida de segurança antiga, muitas organizações não possuem um sistema de *backup* ou o fazem de maneira incorreta. Mesmo no âmbito pessoal, é necessário fazer cópias de seus arquivos.

Montar um sistema de *backup* requer um pouco de cautela. É importante, por exemplo, saber escolher o tipo de mídia para se armazenar as informações.

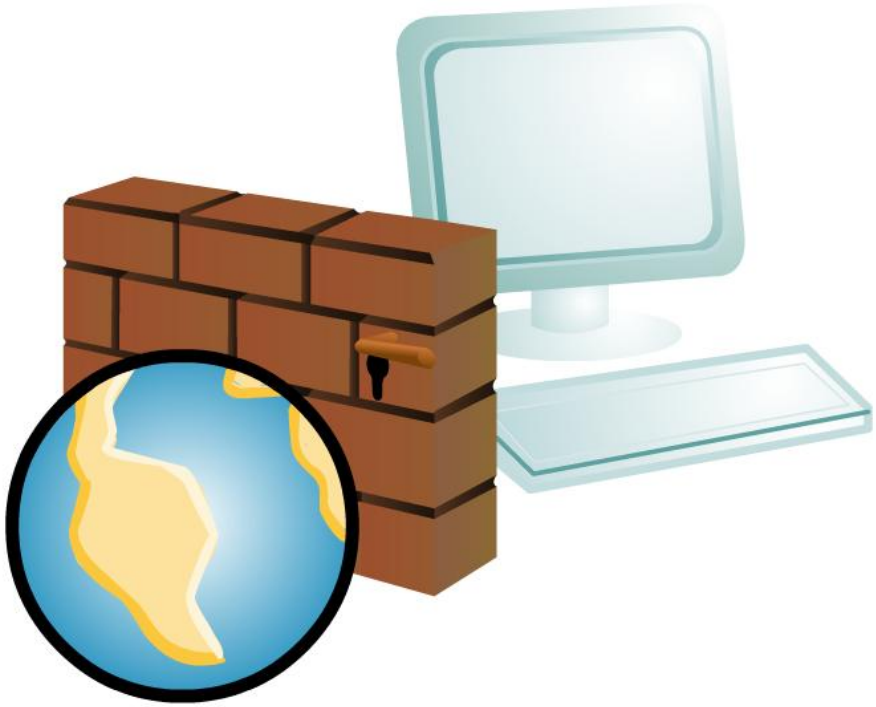
Firewall

Um *firewall* (literalmente: barreira ou parede de fogo) é um sistema cuja função é reforçar a segurança entre duas redes, habitualmente uma rede interna ou Intranet e as redes externas (Internet).

Toda a informação passa pelo sistema, seja para sair ou entrar. É, portanto, a escolha do ponto ideal para colocar filtros, monitorar e verificar ligações e sessões entre estações de trabalho localizadas dentro e fora da rede.

Seus objetivos são:

- ✓ evitar que internautas não-autorizados tenham acesso a computadores, programas, dados e informações não autorizados para o público;
- ✓ proteger a rede interna de ataques de fora (sabotagens, vírus, etc.);
- ✓ impedir que pessoas utilizem a rede interna para promover ataques ao sistema externo;
- ✓ bloquear acesso a determinados *sites*.



Tipos de *firewall*

Os *firewalls* podem vir sob diferentes formatos, abrangendo desde aplicações para computadores individuais até conjuntos de *softwares* que podem ser instalados em estações de trabalho (*workstations*) baseadas em Windows NT ou Unix. Alguns *firewalls* vêm integrados em dispositivos de acesso Internet, tais como Roteadores.

Aplicações do tipo *stand-alone*: ideais para quem já está ligado Internet e não quer substituir os roteadores, ou que precise de um *firewall* com grande capacidade. Estes dispositivos têm duas ligações *Ethernet*, uma para a LAN interna, outra para a ligação WAN/Internet.

Transformando o PC: existem aplicações de *software* que tornam um PC vulgar num *firewall*. Ideais para converter máquinas já integradas na rede num *firewall*. Basta instalar um segundo adaptador Ethernet na máquina. Cuidado, apenas, com a configuração: se for mal feita, pode comprometer a segurança de toda a rede. Faça esta opção apenas se conhecer bem os serviços de rede do sistema operativo no qual será instalado o adaptador.

Integração pré-existente: nos dias atuais, a maior parte dos fabricantes de Roteadores já inclui capacidades de *firewall* nos seus dispositivos. O mesmo produto apresenta, simultaneamente, conectividade Internet e segurança. São dispositivos muito seguros quando configurados corretamente, uma vez que não correm em cima de um sistema operacional. São, geralmente, a melhor opção: fácil e barata.

Você finalizou a segunda aula do terceiro Módulo deste curso.

Nesta aula aprendeu o que é um *hacker* e o que ele pode fazer em relação ao seu computador e suas informações. Estudou os vírus de computador e seus vários tipos de comportamentos assim como os programas de antivírus. Conheceu os s*pywares*, o que eles fazem e como se prevenir. A importância de realizar *backups* periódicos. Teve dicas importantes no momento de criar uma senha mais segura.

Na próxima aula você estudará sobre crime virtual e as leis vigentes sobre o assunto.

Agora, você realizará o Quiz disponibilizado na sequência. Basta responder à algumas questões.

Bom estudo!

Prof. Wagner