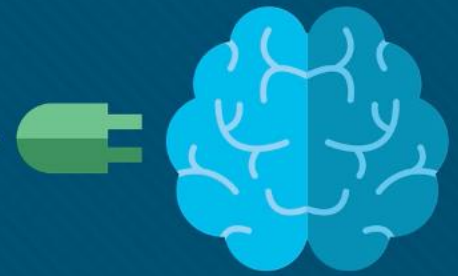


Módulo 3: Protegendo seus Dados e Privacidade

Introdução à Cibersegurança

Objetivos do Módulo

Título do Módulo : Protegendo seus Dados e Privacidade

Objetivo do Módulo: Explique como se proteger enquanto estiver online

Título do Tópico	Objetivo do Tópico
Como proteger a rede e os dispositivos	Identificar as formas de proteger os dispositivos de informática.
Manutenção de dados	Usar redes sem fio com segurança
Quem é o dono dos seus dados?	Criar senhas fortes.
Como proteger a privacidade on-line	Implementar técnicas para manter os dados com segurança.
Descobrir seu próprio comportamento on-line arriscado	Explicar as formas de aumentar a segurança dos dados on-line.

3.1 Protegendo Seus Dispositivos e sua Rede

Protegendo seus Dispositivos e a Rede

- Algumas dicas importantes sobre como proteger a segurança dos dispositivos:

Ative o firewall	Você deve usar pelo menos um tipo de firewall (firewall de software ou de hardware em um roteador) para proteger seu dispositivo contra acesso não autorizado. O firewall deve estar ativado e atualizado constantemente para impedir que hackers acessem seus dados pessoais ou da empresa.
Instalar antivírus e antispyware	Software malicioso, como vírus e spyware, é projetado para obter acesso não autorizado ao seu computador e aos seus dados. Uma vez instalado, os vírus podem destruir os dados e tornar seu computador mais lento. Eles podem até assumir o controle do computador e transmitir e-mails de spam usando a conta. O spyware pode monitorar suas atividades on-line, coletar informações pessoais ou produzir anúncios pop-up indesejados no navegador da Web, enquanto você estiver on-line. Para evitar isso, você só deve baixar software de sites confiáveis. No entanto, ajudaria se você sempre usasse software antivírus para fornecer outra camada de proteção. Este software, que geralmente inclui antispyware, foi projetado para verificar a presença de vírus em seu computador e nos e-mails recebidos e excluí-los.
Gerencie seu sistema operacional e navegador	Os hackers estão sempre tentando tirar vantagem das vulnerabilidades do seu sistema operacional ou navegador da web. Portanto, para proteger o seu computador e os seus dados, você deve definir as configurações de segurança do seu computador e navegador para um nível médio ou superior. Você também deve atualizar regularmente o sistema operacional do seu computador, incluindo o navegador da web, e baixar e instalar os patches de software e atualizações de segurança mais recentes dos fornecedores.
Configurar proteção por senha	Todos os seus dispositivos de computação devem ser protegidos por senha para evitar acesso não autorizado. Qualquer informação armazenada, especialmente dados sensíveis ou confidenciais, deve ser criptografada. Você só deve armazenar as informações necessárias em seu dispositivo móvel, para o caso de ser roubado ou perdido. Lembre-se, se algum dos seus dispositivos for comprometido, os criminosos poderão acessar todos os dados através do seu provedor de serviços de armazenamento em nuvem, como iCloud ou Google Drive.

Segurança de Rede Sem fio em Casa

- As redes sem fio permitem que os dispositivos habilitados para Wi-Fi se conectem à rede por meio de um SSID.
- Um roteador sem fio pode ser configurado para não transmitir o SSID, mas é necessário que haja segurança adequada para uma rede sem fio.
- Os hackers estarão cientes do SSID e da senha padrão predefinidos, portanto, para evitar que invasores entrem na rede sem fio doméstica, você deve alterar esses detalhes.
- Além disso, você pode criptografar a comunicação sem fio ativando a segurança sem fio e o recurso de criptografia WPA2 em seu roteador sem fio.
- Mas esteja ciente de que, mesmo com a criptografia WPA2 habilitada, uma rede sem fio ainda pode ser vulnerável.

- **Descoberta de uma falha de segurança no protocolo WPA2 em 2017**
  - Os ataques de reinstalação de chave (KRACKs) realizados por invasores que quebram a criptografia entre um roteador sem fio e um dispositivo sem fio, dando a eles acesso aos dados de rede, podem explorar essa vulnerabilidade.
  - Essa falha afeta todas as redes Wi-Fi modernas e protegidas e, para mitigar essa situação, você deve:
  - Atualize todos os dispositivos com capacidade sem fio assim que as atualizações de segurança estiverem disponíveis
  - Use uma conexão com fio para qualquer dispositivo com uma NIC com fio
  - Use um serviço VPN confiável ao acessar uma rede sem fio.

Riscos de Wi-Fi Público

- Quando você está longe de casa, pode acessar suas informações online e navegar na Internet por meio de redes sem fio públicas ou pontos de acesso Wi-Fi.
- No entanto, existem alguns riscos envolvidos, o que significa que é melhor não aceder ou enviar informações pessoais através de redes Wi-Fi públicas.
- Ajudaria se você verificasse continuamente que seu dispositivo não está configurado com compartilhamento de arquivos e mídia e requer autenticação de usuário com criptografia.
- Você também deve usar um serviço de VPN criptografado para impedir que outras pessoas interceptem suas informações (conhecidas como "eavesdropping" ou "escutas") em uma rede pública sem fio.
- Este serviço oferece acesso seguro à Internet, criptografando a conexão entre o seu dispositivo e o servidor VPN.
- Mesmo que os hackers interceptem uma transmissão de dados em um túnel VPN criptografado, eles não conseguirão decifrá-la.

Uma Senha Forte

- Aqui estão algumas dicas simples para ajudá-lo na escolha de uma senha forte.

Uso de Uma Frase Secreta

- Ajudaria se você considerasse usar de frase secreta em vez de senhas para evitar acesso não autorizado aos seus dispositivos.
- Uma frase secreta geralmente tem a forma de uma frase ("Acat th@tlov3sd0gs."), tornando mais fácil para você se lembrar.
- E como é mais do que uma senha típica, é menos vulnerável a ataques de força bruta ou de dicionário.
- Aqui estão algumas dicas para criar uma boa senha.

Diretrizes de Senha

- O Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos publicou requisitos de senha aprimorados.
- Os padrões NIST destinam-se a aplicações governamentais, mas também podem servir como padrão para outros setores.
- Essas diretrizes visam atribuir a responsabilidade de verificação de usuário aos provedores de serviços e garantir uma experiência melhor para os usuários em geral.
- Eles afirmam:
  - As senhas devem ter no mínimo oito caracteres, mas não mais que 64 caracteres.
  - Senhas comuns e fáceis de adivinhar, como ‘senha’ ou ‘abc123’, não devem ser usadas.
  - Não devem existir regras de composição, incluindo letras maiúsculas e minúsculas e números
  - Os usuários devem poder ver a senha ao digitar para ajudar a melhorar a precisão.
  - Todos os caracteres e espaços devem ser permitidos.
  - Não deve haver dicas de senha.
  - Não deve haver período de expiração de senha.
  - Não deve haver autenticação baseada em conhecimento, como fornecer respostas a perguntas secretas ou verificar o histórico de transações.

3.2 Manutenção de Dados

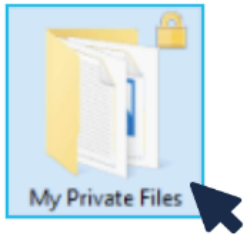
O Que é Criptografia?

- Criptografia é o processo de converter informações em um formato no qual pessoas não autorizadas não possam lê-las.
- Somente uma pessoa confiável e autorizada com uma chave ou senha secreta pode descriptografar os dados e acessá-los em sua forma original.
- Observe que a criptografia em si não impede que alguém intercepte os dados.
- Ele só pode impedir que uma pessoa não autorizada veja ou acesse o conteúdo.
- Alguns criminosos podem criptografar seus dados e torná-los inutilizáveis até que você pague um resgate.

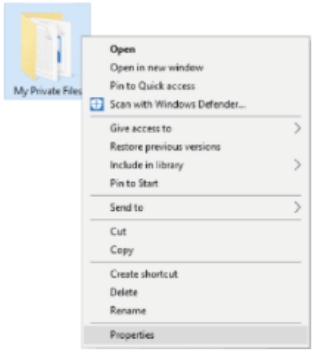
Como Você Criptografa Seus Dados?

- O uso de programas de software serve para criptografar arquivos, pastas e até unidades inteiras.
- EFS é um recurso do Windows que pode criptografar dados. Ele se vincula diretamente a uma conta de usuário específica e somente o usuário que criptografa os dados pode acessá-los após a criptografia usando EFS.
- Como criptografar dados usando EFS em todas as versões do Windows:

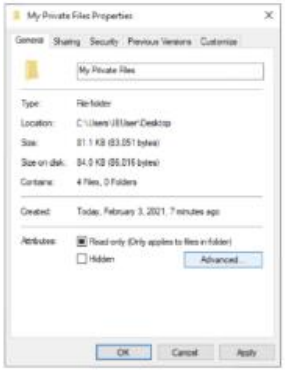
Passo 1
Selecione um ou mais arquivos ou pastas.



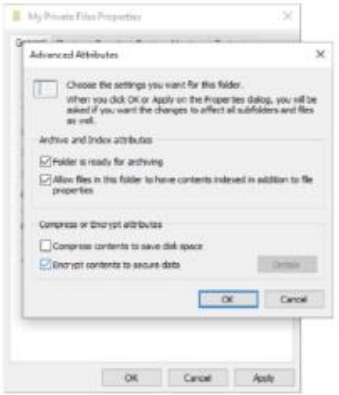
Passo 2
Clique com o botão direito nos dados selecionados e vá para '**Propriedades**'.



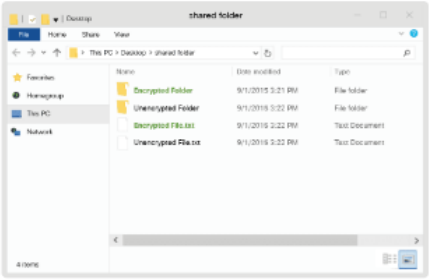
Passo 3
Encontre e clique em '**Avançado**'.



Passo 4
Marque **a caixa de seleção 'Criptografar conteúdo para proteger dados**'.



Passo 5
Arquivos e pastas criptografados com EFS são exibidos em verde.



Backup dos Seus Dados

- Ter um backup pode evitar a perda de dados insubstituíveis.
- Para fazer backup dos dados corretamente, você precisará de um local de armazenamento adicional e deverá copiar os dados para esse local regularmente.

Alguns destes locais de armazenamento adicionais:

Rede residencial	Armazenar seus dados localmente significa que você tem controle total sobre eles.
Local secundário	Você pode copiar todos os seus dados para um NAS, um disco rígido externo simples ou talvez até fazer backup de pastas importantes em pen drives, CDs, DVDs ou fitas. Neste cenário, você é o proprietário dos dados e é responsável pelo custo e pela manutenção do equipamento do dispositivo de armazenamento.
A nuvem	Você poderia assinar um serviço de armazenamento em nuvem, como AWS. O custo deste serviço dependerá do espaço de armazenamento necessário, portanto, talvez seja necessário ser mais seletivo quanto aos dados dos quais você faz backup. Você terá acesso aos seus dados de backup contanto que tenha acesso à sua conta. Um dos benefícios de usar um serviço de armazenamento em nuvem é que seus dados estão seguros no caso de falha de um dispositivo de armazenamento ou se você enfrentar uma situação extrema, como um incêndio ou roubo.

Como Você Exclui Seus Dados Permanentemente?

- Você já teve que excluir dados ou se livrar de um disco rígido?

- Em caso afirmativo, você tomou alguma precaução para proteger os dados e evitar que caiam em mãos erradas?

- O que você deve fazer para garantir a exclusão de seus arquivos de forma segura e permanente?
  - Para apagar dados, de modo que não sejam mais recuperáveis, eles devem ser substituídos por uns e zeros várias vezes, usando ferramentas projetadas especificamente para fazer exatamente isso.
  - SDelete da Microsoft afirma ter a capacidade de remover completamente arquivos confidenciais.
  - Shred para Linux e Secure Empty Trash para Mac OS X afirmam fornecer um serviço semelhante.
  - A única maneira de garantir que os dados ou arquivos não sejam recuperáveis é destruir fisicamente o disco rígido ou dispositivo de armazenamento.
  - Muitos criminosos se valeram de arquivos considerados impenetráveis ou irrecuperáveis!

3.3 Quem é o Dono dos Seus Dados?

Compreensão Dos Termos

- Os Termos de Serviço incluirão algumas seções, desde direitos e responsabilidades do usuário até isenções de responsabilidade e termos de modificação de conta.

- A política de uso de dados descreve como o provedor de serviços coletará, usará e compartilhará seus dados.

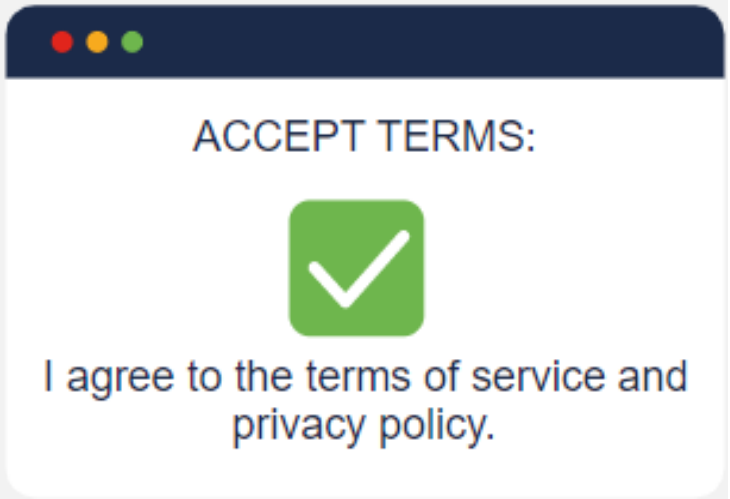
- As configurações de privacidade permitem controlar quem vê informações sobre você e quem pode acessar seus dados de perfil ou de conta.

- A política de segurança descreve o que a empresa está fazendo para proteger os dados obtidos de você.

O que Você Está Concordando?

- Você criou a conta @Apollo e concordou com os Termos de Serviço da empresa de compartilhamento de fotos on-line.

- Mas você realmente sabe pelo que se inscreveu?



Antes de se Inscrever

- Quais fatores você deve considerar antes de se inscrever em um serviço on-line?
- Você já leu os Termos de Serviço?
- Quais são os seus direitos em relação aos seus dados?
- Você pode solicitar uma cópia de seus dados?
- O que o provedor pode fazer com os dados dos quais você fez upload?
- O que acontece com seus dados depois que você fecha sua conta?

3.4 Como Proteger a sua Privacidade on-line

Autenticação de Dois Fatores

- Serviços on-line populares, como Google, Facebook, Twitter, LinkedIn, Apple e Microsoft, usam autenticação de dois fatores para adicionar uma camada extra de segurança nos logins de conta.

- Além de seu nome de usuário e senha ou número de identificação pessoal (PIN), a autenticação de dois fatores requer um segundo token para verificar sua identidade.

- Pode ser:
  - objeto físico, como um cartão de crédito, telefone celular ou fob (chave de segurança)
  - varredura biométrica, como impressão digital ou reconhecimento facial e de voz
  - código de verificação enviado por SMS ou e-mail.

Autorização Aberta ou Open Authorization

- Open authorization (OAuth) é um protocolo padrão aberto que permite que você use suas credenciais para acessar aplicativos de terceiros sem expor sua senha.
- O que isso significa na prática?
- Você está ansioso para se inscrever no curso de segurança da Cisco “Cybersecurity Essentials”, desta série, para ajudá-lo a desenvolver sua carreira. Mas você deve estar conectado ao portal de eLearning para fazer isso.

- Você não consegue se lembrar dos detalhes de login, mas tudo bem. O portal permite que você faça login usando suas credenciais de um site de mídia social como o Facebook ou de outra conta como o Google.

- Portanto, em vez de redefinir seus dados de login, você pode fazer login facilmente no portal de eLearning usando suas contas de mídia social existentes e se inscrever no próximo curso. Você não se aguenta para começar logo!

Vídeo – Não Seja Enganado

Um simples e-mail falsificado ou falsificado pode levar a uma violação de dados enorme e talvez causar danos irreversíveis à sua reputação.

Privacidade de e-mail e Navegador da Web

- Esses problemas podem ser minimizados ativando o modo de navegação privada em seu navegador.
- Muitos dos navegadores mais usados têm seu nome para modo de navegador privado:
  - **Microsoft Internet Explorer:** InPrivate
  - **Google Chrome:** Incognito
  - **Mozilla Firefox:** Private tab or private window
  - **Safari:** Private browsing

- Como funciona o modo privado?
  - Quando o modo privado está ativado, os cookies, arquivos salvos em seu dispositivo para indicar quais sites da Web visitados, são desativados.
  - Portanto, remova todos os arquivos temporários da Internet e exclua seu histórico de navegação ao fechar a janela ou programa.
  - Isso pode ajudar a evitar que outras pessoas coletem informações sobre suas atividades on-line e o incentivem a comprar algo com anúncios direcionados.
  - Mesmo com a navegação privada ativada e os cookies desativados, as empresas estão constantemente a desenvolver novas formas de recolher impressões digitais dos utilizadores para monitorizar o seu comportamento online.

3.5 Descobrir seu Próprio Comportamento de Risco on-line

3.6 Questionário do Módulo

O Que Aprendi Neste Módulo?

- É importante proteger a segurança dos seus dispositivos.
- Algumas dicas para fazer isso são: ativar o firewall, instalar antivírus e anti-spyware, gerenciar o navegador do sistema operacional e configurar a proteção por senha.
- O SSID predefinido e a senha padrão devem ser alterados para evitar que intrusos entrem na sua rede sem fio doméstica.
- Além disso, ajudaria se você criptografasse a comunicação sem fio ativando a segurança sem fio e o recurso de criptografia WPA2 em seu roteador sem fio.
- Mas mesmo com a criptografia WPA2 habilitada, uma rede sem fio ainda pode ser vulnerável.
- É melhor não acessar ou enviar qualquer informação pessoal ao usar uma rede Wi-Fi pública.
- Ajudaria se você verificasse continuamente se o seu dispositivo configura o compartilhamento de arquivos e mídia e requer autenticação do usuário com criptografia.
- Você também deve usar um serviço VPN criptografado para evitar que outras pessoas interceptem suas informações em uma rede sem fio pública.
- Sempre use senhas fortes, sem usar senhas com erros ortográficos de palavras comuns do dicionário e caracteres especiais e senhas com mais de dez caracteres.
- Você deve considerar o uso de senhas.
- Criptografia é o processo de converter informações em um formato no qual pessoas não autorizadas não possam lê-las.
- A criptografia em si não impede que alguém intercepte os dados.
- Ele só pode impedir que uma pessoa não autorizada veja ou acesse o conteúdo.

O Que Aprendi Neste Módulo? (Cont.)

- O uso de programas de software serve para criptografar arquivos, pastas e até unidades inteiras.
- O EFS (Encrypting File System, Sistema de Criptografia de Arquivos) é uma característica do Windows que pode criptografar dados.
- Ter um backup pode evitar a perda de dados insubstituíveis.
- Alguns locais de armazenamento são a rede doméstica, o local secundário e a nuvem.
- Para apagar dados, de modo que não sejam mais recuperáveis, eles devem ser substituídos por uns e zeros várias vezes, usando ferramentas projetadas especificamente para fazer exatamente isso.
- No entanto, a única maneira de garantir que os dados ou arquivos não sejam recuperáveis é destruir fisicamente o disco rígido ou dispositivo de armazenamento.
- Os Termos de Serviço incluirão algumas seções, desde direitos e responsabilidades do usuário até isenções de responsabilidade e termos de modificação de conta.
- Considere alguns fatores antes de se inscrever em um serviço on-line, como lê-lo e conhecer seus direitos.
- Em relação aos seus dados, se você pode ou não solicitar uma cópia dos seus dados, entre outros.
- Serviços online populares como Google e Facebook usam autenticação de dois fatores para adicionar uma camada extra de segurança para logins de contas.
- Open authorization (OAuth) é um protocolo padrão aberto que permite que você use suas credenciais para acessar aplicativos de terceiros sem expor sua senha.
- Um simples e-mail forjado ou falsificado pode levar a uma violação massiva de dados e causar danos irreversíveis à sua reputação.
- Esses problemas podem ser minimizados ativando o modo de navegação privada em seu navegador.