Segurança cibernética, fraude eletrônica e spam

Os participantes aprenderão sobre usuários online mal-intencionados que podem tentar usar vulnerabilidades de segurança para colher informações sobre eles. Os participantes poderão descrever os riscos de se estar online, desenvolver estratégias para condutas mais seguras, identificar mensagens de spam e explicar quem poderia solicitar suas senhas.

Materiais

- Spam

Riscos online

Parte 1

Fale para seus alunos

Ao usar a Internet, você pode se expor a riscos pelo simples ato de acessar uma página da web, comunicar-se online ou baixar dados. Às vezes é possível que sites acessados, pessoas na mesma rede ou até terceiros consigam descobrir sua localização ou outras informações sobre você durante sua navegação.

Pergunte aos seus alunos

Quem pode tirar proveito de vulnerabilidades de segurança online para ver suas informações pessoais?

1. Possíveis respostas incluem hackers mal-intencionados, vigilância governamental e outros.

Fale para seus alunos

Ao navegar pela web, é possível que hackers mal-intencionados coletem dados sobre você da mesma forma que os provedores de Internet fazem. Para reduzir esse risco, use uma conexão segura entre você e os sites que está tentando acessar. Independentemente de sua conexão, muitos sites tentam rastrear seus padrões de uso em várias plataformas. Eles podem acompanhar seu navegador, sua localização e outros padrões de uso para tentar descobrir quem você é.

Pergunte aos seus alunos

Por que hackers mal-intencionados poderiam tentar acessar suas informações online? Que informações essas pessoas estão procurando? Por que um site ao qual você não está conectado gostaria de rastrear quem você é?

1. Por informações de identificação pessoal e outras que possam ser vendidas ou utilizadas para ganhos financeiros.

Alguém sabe o que é malware? O que ele faz?

Fale para seus alunos

Malware é código mal-intencionado executado de forma oculta em seu computador. Alguns malware podem coletar dados de qualquer parte de seu computador local, do disco rígido aos dados de navegador. Eles também podem permitir que hackers

tomem controle de seu computador e o utilizem como quiserem. A maioria dos malware são mais simples, como sites que imitam portais seguros, como o de um banco, ou extensões que colocam anúncios em seu navegador para ganhar dinheiro.

Pergunte aos seus alunos

O que você pode fazer para se proteger de malware, espionagem ou rastreamento?

Fale para seus alunos

Cuidado ao clicar em links, anúncios ou publicações de redes sociais. A URL corresponde ao que você queria? Você acessa a mesma página que aparece ao digitar a URL ou pesquisar o site? Uma boa regra é que SSL/TLS deve proteger a página de login de qualquer conta importante (como Google, Facebook, Twitter ou contas bancárias). SSL/TLS dificulta o processo de um hacker na mesma rede enviar um site falso a você caso digite a URL correta, o que seria bem fácil sem esse protocolo.

Alguns sites poderão executar código para acessar suas informações pessoais ou contas online se errarem no código. Eles podem usar suas contas para gerar spam para outras pessoas.

Somente baixe ou instale software de fontes confiáveis e tenha cuidado na hora de baixar arquivos executáveis (extensões .exe, .pkg, .sh, .dll ou .dmg). Executáveis são arquivos que executam uma ação. Às vezes, essas ações podem ser ruins. Por exemplo, alguém pode escrever um executável para apagar o disco rígido de outra pessoa ou instalar um navegador falso. É por isso que você só deve instalar conteúdo de fontes confiáveis.

Você pode usar software antivírus para evitar a execução de malware. Alguns software antivírus vêm com o computador (por exemplo, o Microsoft Security Essentials para Windows); já outros sistemas operacionais, como os dos computadores Apple, têm configurações de segurança que bloqueiam a instalação de software de fontes não confiáveis. Pense bem antes de ignorar essas configurações.

Pense em usar também extensões de navegador que podem, por exemplo, bloquear plug-ins, dificultando o rastreamento por sites. No entanto, esse mesmo plug-in pode bloquear funções dos sites, como a capacidade de veicular vídeos. Você é que decide se quer instalar extensões de navegador de acordo com suas preferências e os riscos que aceita correr em termos de segurança online. Pense no grau de inconveniência que o rastreamento gera para você ou não. Qual é o valor de minha privacidade? Quero assistir a esse conteúdo (se, por exemplo, a extensão do navegador bloquear um plug-in que processa o vídeo) tanto assim?

Ferramentas de segurança

Parte 1

Interação da classe

Observação: parte do conteúdo dessa atividade foi abordada na “Atividade 1: Riscos online” Você decide se quer rever o material, caso já tenha percorrido a Atividade 1, ou ignorá-lo.

Pergunte aos seus alunos

Você sabe se está protegido quando usa a Internet?

Fale para seus alunos

Sem tomar os cuidados necessários, pode ser difícil ou até impossível se proteger contra esses riscos online (os descritos na seção anterior).

Outros riscos online podem surgir a qualquer momento e, portanto, é importante estar sempre atento.

Pergunte aos seus alunos

O que uma pessoa poderia fazer se convencesse você de que o site dela é importante?

Existem ferramentas que você pode usar para evitar ou diminuir esses riscos. Alguém conhece alguma?

Fale para seus alunos

HTTPS é um padrão usado por sites para criptografar dados transmitidos pela internet. A criptografia pode evitar que terceiros visualizem dados de sua conexão. Ela oferece uma camada adicional de segurança e pode ser usada em qualquer navegador com a adição de “http://” na frete da URL utilizada (por exemplo, https://www.mysite.com). No entanto, nem todos os sites aceitam HTTPS.

1. Insira informações confidenciais (por exemplo, senhas, informações de cartão de crédito) apenas em páginas da web com prefixo HTTPS://.

2. É possível usar ferramentas de software para garantir o uso de HTTPS sempre que possível.

3. A maioria dos navegadores têm indicadores de segurança em formato de cadeado ao lado da barra de endereços para indicar as conexões HTTPS.

4. Infelizmente, HTTPS não garante segurança total, já que alguns sites mal-intencionados também aceitam HTTPS. O HTTPS protege a conexão, mas não é garantia de que o site seja genuíno.

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) são os nomes das tecnologias que protegem o HTTPS. SSL/TLS usam chaves de criptografia, que funcionam de forma bem semelhante a chaves reais. Se você escrever um segredo em um pedaço de papel para seu amigo, quem encontrar o papel verá seu segredo. Mas e se você der a ele uma cópia da chave pessoalmente e enviar o segredo em caixas trancadas iguais? Se alguém interceptar a caixa, terá dificuldade em ver o segredo sem a chave. Se alguém tentar substituir a caixa por uma semelhante, você notará se a chave funciona ou não. O SSL/TLS funciona da mesma maneira, mas em um site.

Os indicadores de segurança do navegador também comunicarão as informações de certificado de Validação Estendida (EV). Os certificados EV são conferidos a sites que confirmam suas identidades junto a uma autoridade certificada. Nos navegadores, o indicador de EV às vezes tem o formato do nome do site ou da entidade de registro ao lado da barra de endereços. Os certificados EV são conferidos a sites que confirmam suas identidades junto a uma autoridade certificada. Nos navegadores, o indicador de EV às vezes tem o formato do nome do site ou da entidade de registro ao lado da barra de endereços. Se você suspeita do conteúdo de um site específico, verifique se a URL no certificado está de acordo com a URL no navegador clicando em “Visualizar certificado”. (Pode ser útil demonstrar como encontrar “Visualizar certificado” na tela de projeção.) Esses passos variam de acordo com o navegador. Por exemplo, no Chrome, em “Visualizar”, clique em “Desenvolvedor” e em “Ferramentas para desenvolvedores”. Em “Ferramentas para desenvolvedores”, clique na guia “Segurança” e em “Visualizar certificado”.

Além do fato de não executar software de fontes não confiáveis, um software antivírus pode impedir que você visite páginas não confiáveis ou baixe malware.

O ato de “fraude eletrônica” ocorre principalmente por emails enviados por remetentes de spam que se fazem passar por remetentes legítimos. Eles pedem sua senha e esperam que você vá enviá-la por email ou entrar em um site falso. Os filtros de spam podem evitar que alguns desses emails cheguem à caixa de entrada. Para melhorar os filtros de spam, marque sempre emails suspeitos que apareçam na caixa de entrada como spam.

Pergunte aos seus alunos

Que medidas você tomaria para evitar baixar acidentalmente arquivos que possam prejudicar seu computador?

Fale para seus alunos

Confira sempre se está baixando arquivos de sites confiáveis. Tome muito cuidado na hora de abrir anexos de emails não conhecidos e de clicar em janelas pop-up e mensagens de erro. Pense também em instalar programas contra malware reconhecidos no computador.

Como compartilhar senhas

Parte 1

Pergunte aos seus alunos

Em que situações não há problemas em divulgar a senha?

1. Possíveis respostas incluem contas compartilhadas (por exemplo, Netflix).

Quais riscos podem estar associados à divulgação da senha?

1. Se uma pessoa mal-intencionada obtém sua senha, sua conta pode ser invadida. A divulgação da senha aumenta a chance de alguém obter acesso a ela. Se a mesma senha é usada em outros sites, ela também pode ter acesso a esses sites.

Fale para seus alunos

A prática comum é a de não divulgar senhas a ninguém além do aplicativo que a exige para login. Como descrito anteriormente, fraude eletrônica é o ato de enganar alguém para que divulgue sua senha.

No entanto, algumas pessoas podem pedir sua senha explicitamente para poder acessar suas contas dizendo que elas podem estar em perigo. Embora algumas dessas pessoas possam ter boas intenções, como um amigo que deseja ajudá-lo a examinar sua conta, não é boa ideia divulgar a senha, especialmente se ela é usada em várias contas. Se você pretende divulgar a senha, verifique se ela não é usada em nenhuma outra conta e use um gerenciador de senhas para compartilhar o acesso.

Às vezes, a pessoa que pede a senha pode ser um adulto conhecido e confiável, como seus pais, professores ou empregador. Embora você conheça e confie nesses adultos, normalmente é melhor para todos (as duas partes envolvidas) ter uma conversa sobre o motivo desse pedido e sobre como eles lidarão com sua senha. Quando são adultos de fora da família, é uma boa ideia perguntar a eles diretamente se há alguma lei ou regra que exija esse tipo de divulgação.

Fazer perguntas claras e educadas sobre leis e regras é particularmente importante quando a solicitação de senha vem de um adulto que não é da sua família e que você não conhece pessoalmente, como um policial. Se um policial ou outra autoridade governamental pedir a senha de suas redes sociais, fique calmo e mantenha o respeito. Pergunte por que ele pede isso e que leis ou regras fundamentariam esse pedido.

Dependendo das circunstâncias de uma solicitação feita por pais/tutores, professores, empregador, policiais, autoridade governamental ou outro pessoa adulta, pode ser que você tenha que divulgar sua senha. As circunstâncias que exigiriam isso envolvem alguma lei ou regra que estabeleça essa divulgação ou seu bom senso na hora de avaliar se a ajuda dessas pessoas é mais benéfica do que o risco causado pela divulgação da senha.

Caso um adulto peça sua senha e esse pedido cause algum desconforto, fale com um de seus pais/tutores ou outro adulto de confiança imediatamente, especialmente antes de ter que responder ao pedido.

Pergunte aos seus alunos

Em que circunstâncias você deveria divulgar sua senha online?

1. Somente quando é solicitado pelo site que você está tentando acessar. Nunca compartilhe sua senha em outros lugares, inclusive por email, pois não costuma estar criptografado ou protegido.

Tarefa

Folheto

Atribuição

Divida os participantes em grupos de 2 a 3 pessoas. Distribua o folheto de participante sobre spam. Em seguida, peça a cada participante para criar um fluxograma que mostre como eles podem identificar spam e se devem divulgar determinadas informações com outras pessoas/grupos de pessoas.

Fale para seus alunos

Leia cada um dos cenários e converse sobre a possibilidade de serem spam e se vocês compartilhariam informações com a pessoa ou o grupo de pessoas envolvido no cenário.

Interação da classe

Dê aos participantes 10 minutos para isso. Em seguida, peça aos grupos para mostrarem suas respostas.

Pergunte aos seus alunos

Quando você deve compartilhar a senha por email?

Fale para seus alunos

É prática comum entre sites e empresas nunca pedir sua senha por email. Nunca transmita sua senha a ninguém dessa maneira, mesmo que a fonte pareça legítima. Os emails quase nunca são protegidos.

Parte 2

Atribuição

Desmembre os grupos, já que o exercício a seguir é individual.

Dê aos participantes 15 minutos para que criem seus fluxogramas.

Fale para seus alunos

Agora, em um pedaço de papel, crie um fluxograma para mostrar às pessoas como elas podem identificar spam e se podem compartilhar determinadas informações online com outras pessoas. Pode ser útil usar um cenário específico como base para o fluxograma, seja um dos cenários do folheto ou um novo (se for um dos

cenários do folheto, indique o número do cenário em cima do fluxograma). Caso escolha criar seu próprio cenário, descreva-o em um parágrafo curto acima do fluxograma.

Dê aos participantes 15 minutos para que criem seus fluxogramas.