Senhas

Os participantes aprenderão a proteger melhor suas informações online usando e mantendo senhas fortes. Os participantes aprenderão os princípios de criação de senhas fortes e os possíveis problemas na divulgação de senhas. Eles também aprenderão a proteger as senhas e a tomar medidas para evitar o acesso não autorizado às contas.

Materiais

- Aprendizado sobre senhas

Noções básicas de senha

Parte 1

Fale para seus alunos

Normalmente, não pensamos muito sobre como usamos senhas em sites, aplicativos e serviços. No entanto, a força de uma senha determina a segurança das informações protegidas.

Interação da classe

Envolva os participantes em um debate sobre as perguntas a seguir. Lembre a eles de que é importante não divulgar suas senhas reais durante este ou qualquer outro exercício.

Pergunte aos seus alunos

Quantas senhas você tem?

> Você tem senhas diferentes para sua conta de email e suas contas de redes sociais?
>
> Elas são muito diferentes ou são uma variante da mesma senha?

Caso tenha mais de uma senha, como você se lembra qual serve para cada conta?

Pergunte aos seus alunos

Com que frequência você esquece uma senha importante?

> O que você fez quando esqueceu a senha?
>
> Como você torna suas senhas fáceis de lembrar?

Existe alguma senha que você use todos os dias?

O que aconteceria se alguém descobrisse sua senha sem que você soubesse?

> Dependeria de quem fosse?

Que tipo de informações alguém poderia descobrir sobre você se usasse a senha para entrar em sua conta?

Parte 2

Interação da classe

Organize os participantes em duplas.

Fale para seus alunos

Junto com seu parceiro, fale sobre o que aconteceria se alguém que queira causar problemas descobrisse a senha de sua plataforma de redes sociais favorita.

Interação da classe

Dê aos participantes 5 minutos para debaterem. Peça aos grupos para que compartilhem suas conclusões.

Fale para seus alunos

Agora, converse com seu parceiro sobre o que aconteceria se um hacker descobrisse a senha da internet da conta bancária de seus pais ou tutores.

Interação da classe

Dê aos participantes 5 minutos para debaterem. Em seguida, peça aos grupos para que compartilhem suas conclusões.

Parte 3

Fale para seus alunos

Você talvez esteja se perguntando como um hacker poderia descobrir uma senha privada. Existem algumas maneiras: uma é por meio de engenharia social, ou enganar alguém para que revele sua senha. Um hacker pode fazer isso enviando um email que parece legítimo de uma plataforma ou site onde a pessoa tem uma conta. O email pode pedir que a pessoa clique em um link e entre com o nome de usuário e a senha; quando a pessoa faz isso, essas informações ficam disponíveis para o hacker.

Às vezes, os hackers tentam adivinhar senhas usando termos comuns, como “senha123”, “teste” ou seu nome ou sobrenome.

Outra maneira de descobrir uma senha privada é pelo que se chama ataque de “força bruta”. Um ataque de força bruta ocorre quando um hacker tenta entrar em sua conta tentando adivinhar várias senhas repetidamente. Embora um hacker possa fazer um ataque de força bruta manualmente, isso costuma ser feito por um programa de computador que tenta automaticamente e com rapidez todas as

combinações de senha possíveis. Por exemplo, uma lista de senhas possíveis ou um conjunto de senhas que são combinações de letras e números diferentes, até conseguir encontrar a senha certa.

É claro que alguns ataques de força bruta são mais sofisticados. Se sua senha está em uma lista de possíveis senhas, como “pingo123” ou “senha”, alguns programas podem adivinhar mais rapidamente tentando essas opções antes de outras menos prováveis ou de opções criadas aleatoriamente. O ataque também pode ser mais sofisticado se o hacker tiver informações sobre você. Se o hacker sabe que o nome de seu animal de estimação é Luna, pode tentar “Luna” com várias combinações de números no final (por exemplo, “Luna629” ou “Luna3020”).

Princípios de design

Parte 1

Pergunte aos seus alunos

Quem sabe o que significa ter uma senha “forte” ou “mais forte”? Por que isso é uma boa ideia?

Fale para seus alunos

Uma senha forte ajuda a proteger suas informações. Embora a senha forte não possa garantir que a conta não será invadida, uma senha fraca facilita o acesso às informações por outras pessoas.

Exercício de senha

Pergunte aos seus alunos

Deem alguns exemplos de senhas fracas.

1. Alguns exemplos incluem: senha, 12345, Olá!, data de nascimento, apelido.

Por que você acha que essas senhas são fracas?

1. Elas podem ser adivinhadas por outra pessoa e/ou computador facilmente por meio de um ataque de força bruta.

Como você pode tornar a senha mais forte?

1. Adicionando números, símbolos e letras em maiúsculas e minúsculas, tornando a senha mais longa e evitando usar somente palavras e expressões comuns.

Interação da classe

Quando os participantes terminarem de dar suas opiniões, escreva essas instruções no quadro:

Incluir pelo menos um número.

Incluir pelo menos um símbolo.

Incluir pelo menos uma letra em maiúscula e uma em minúscula.

As senhas devem conter no mínimo 7 caracteres.

As senhas devem ser fáceis de lembrar (a menos que você use um gerenciador de senhas).

Gerenciador de senhas é um site/aplicativo que ajuda usuários a salvar e organizar suas senhas.

As senhas não devem ser uma palavra comum ou informação pessoal (data de nascimento, nome de um dos pais e afins).

Elas não devem ser usadas em sites diferentes.

Fale para seus alunos

Existem duas abordagens para se criar senhas fortes. A primeira é seguir uma "receita de senha", como a mostrada no quadro. O uso dessa receita ajuda você a incluir elementos mais difíceis de se adivinhar em uma senha alfanumérica, impedindo que ela seja descoberta casualmente. O problema dessa abordagem é que ela torna as senhas mais difíceis de lembrar.

Senhas fortes

Fale para seus alunos

Outra abordagem para criar senhas fortes diz respeito ao tamanho da senha. Como a força da senha está relacionada com seu tamanho, o uso de uma cadeia de quatro ou mais palavras não relacionadas dificultam muito mais a adivinhação da senha por humanos ou em ataques de força bruta. Esse método tem outra vantagem de resultar em senhas mais fáceis de se lembrar do que pelo método da receita.

Por fim, é possível usar uma combinação desses dois métodos criando uma cadeia de quatro ou mais palavras não relacionadas com símbolos e números.

O objetivo desses métodos é o mesmo: criar senhas que sejam exclusivas e difíceis de se adivinhar.

Fale para seus alunos

Organize os participantes em duplas

Em duplas, tentem criar uma senha forte usando as instruções escritas no quadro. Lembre-se de que uma senha que um computador não consegue adivinhar aleatoriamente com facilidade pode ainda ser fácil para um humano ou computador

com uma lista de senhas longas comuns. O pedaço de papel com sua senha não será recolhido no final da atividade. Não use essa senha em uma de suas contas, já que os que estão em seu grupo a conhecem.

Dê aos participantes 5 minutos para essa atividade. Em seguida, percorra a sala e pergunte aos participantes quais exemplos são os mais fortes. Pergunte a eles se conseguem lembrar das senhas geradas sem olhar diretamente para o papel.

Embora alguns sites exijam algumas condições (ou todas) para a criação da senha, outros não têm essas restrições. Você também pode criar senhas usando uma cadeia de palavras aleatórias comuns.

Interação da classe

Em duplas, os participantes criam novas senhas que são sequências de palavras. Informe-os que a senha deve ter pelo menos quatro palavras para que seja forte e fácil de lembrar. Dê aos participantes 5 minutos para essa atividade. Em seguida, percorra a sala e peça para os participantes compartilharem seus exemplos de senhas. Lembre novamente os participantes que a folha de papel não será coletada no final da atividade, nem a senha deve ser usada para suas contas.

Fale para seus alunos

Alguns sites usam um sistema chamado autenticação multifator (ou de dois fatores) para verificar sua identidade. Esses sites costumam usar mensagens de texto, aplicativo ou email a fim de enviar um código avulso para ser inserido com a senha.

Esse método pode proteger ainda mais suas contas ao adicionar uma camada extra de segurança que é mais difícil de ultrapassar. Por exemplo, para entrar na conta, uma pessoa precisa ter sua senha e acesso ao aplicativo, dispositivo ou endereço de email associado a ela.

Como manter as senhas protegidas

Parte 1

Fale para seus alunos

Mesmo que você crie uma senha realmente difícil de ser descoberta por um computador ou por uma pessoa, outros fatores podem torná-la fraca.

Pergunte aos seus alunos

Como as senhas podem ser fracas?

1. Dentre alguns exemplos, temos: reutilizar a senha em várias contas, usar uma senha com informações pessoais, usar a mesma senha por vários anos, esquecer sua senha.

Com que frequência você acha que deve mudar as senhas?

Fale para seus alunos

Mesmo senhas muito boas podem ficar comprometidas ou estar sujeitas a roubo, mas há maneiras de se proteger. Se houver vazamento de dados em um site onde você tem conta, mude sua senha nesse site e em outros sites cujas senhas sejam parecidas.

É difícil ter que lembrar de várias senhas complexas.

Pergunte aos seus alunos

Você não acha que é uma boa ideia anotar as senhas em um pedaço de papel ou em um arquivo de documentos no computador? Por que sim ou por que não?

Interação da classe

Mencione possibilidades, como alguém encontrar o pedaço de papel ou notar o arquivo no computador. Explique que uma das abordagens é usar um gerenciador de senhas, aplicativo que ajuda usuários a salvar e organizar suas senhas.

Parte 2

Fale para seus alunos

Todos os dias, usamos várias contas diferentes em sites diferentes. Pode ser complicado entrar e sair de todos os sites a cada sessão.

Pergunte aos seus alunos

Você já usou o recurso “salvar senha” em seu navegador para salvar a senha de um site? Por que sim ou por que não?

Você sabe como o site se lembra de cada usuário?

1. Peça explicações. Em seguida, explique que os sites podem se lembrar dos usuários pelo armazenamento de cookies. Cookies são pequenos arquivos armazenados em seu computador para ajudar um site a saber quem você e seu computador são em visitas posteriores, sem a necessidade de um novo login. No entanto, os cookies também podem ser usados para rastreá-lo quando você passeia entre sites. Essa é uma das formas usadas pelos anúncios para direcionamento.

Há algum problema em salvar uma senha em seu próprio computador?

Pergunte aos seus alunos

Seu computador tem uma senha para login?

E se você compartilhar o computador com outras pessoas?

1. Nesse caso, mesmo que a senha no campo de senha esteja oculta por pontos pretos ou asteriscos, outras pessoas que usam seu computador podem descobri-la. Não conseguir ver a senha na tela não quer dizer que ela não esteja armazenada em algum lugar.

Pergunte aos seus alunos

Existem situações em que não há problema em compartilhar senhas? Quando? Por quê?

1. Alguns exemplos incluem quando os pais querem ter as senhas de seus filhos ou quando eles têm uma conta conjunta/familiar em um serviço como o Netflix.

Você compartilha suas senhas com alguém? Se sim, com quem e por quê?

Se algum amigo próximo disser “se você se importa comigo”, isso seria um incentivo para você divulgar sua senha para ele? Por que sim ou por que não?

Fale para seus alunos

Você pode optar por divulgar sua senha para alguém com quem se importe, mas

gostar de alguém não significa necessariamente que essa pessoa mereça ter acesso total a suas contas online.

Pense bem sobre seu relacionamento com essa pessoa antes de divulgar a senha; pense inclusive em como esse relacionamento pode mudar ao longo do tempo. Por exemplo, divulgar a senha para pais ou tutores é bem diferente de divulgar para seu(sua) melhor amigo(a).

Pergunte aos seus alunos

O que poderá acontecer com você se resolver divulgar a senha?

1. Alguém pode entrar em suas contas bancárias, se fazer passar por você online ou descobrir alguns de seus segredos.

Se você divulgasse a senha de uma conta, usaria essa conta de maneira diferente?

Pergunte aos seus alunos

Existem coisas que você não assistiria no Netflix ou escreveria em um email se alguém mais pudesse ver essas ações?

Interação da classe

Os participantes devem refletir sobre seus comportamentos na hora de usar uma conta compartilhada. Eles devem pensar que suas atividades online estão visíveis pra outros usuários da conta.

Pergunte aos seus alunos

Se sua conta é uma representação virtual de você, como um perfil de redes sociais, há problema em permitir que outros usuários a utilizem?

Interação da classe

Debata a possibilidade de alguém se fazer passar por você e enviar mensagens para seus amigos.

Pergunte aos seus alunos

Você permite que alguns de seus dispositivos armazenem as senhas? Por que sim ou por que não? Isso significa que é seguro salvar senhas em seu celular ou computador pessoal? O que poderia acontecer se você emprestasse seu telefone ou computador para um amigo?

Existem dispositivos que você compartilha com outras pessoas, como familiares ou

amigos? Você compartilha alguma conta nesse dispositivo? Ou cada pessoa tem uma?

Você usa dispositivos “públicos”, como um de uma biblioteca, do colégio ou de outro lugar? Você faz as mesmas coisas que faria em outros lugares nesse dispositivo?

Parte 3

Interação da classe

Organize os participantes em duplas.

Fale para seus alunos

Em duplas, conversem sobre a experiência de fazer login em um computador no colégio, em uma biblioteca ou em outra situação pública e encontrar o perfil de outra pessoa ainda conectado às redes sociais ou à conta de email. Pergunte a eles se eles dariam uma olhada na conta ou fariam outra coisa.

Interação da classe

Dê aos participantes 5 minutos para debaterem o assunto e peça a eles para que compartilhem suas conclusões. Envolva o grupo em um debate sobre esse uso não autorizado.

Acesso não autorizado à conta

Parte 1

Interação da classe

Observação: parte do conteúdo dessa atividade foi abordada na “Atividade 1: Noções básicas de senha” Você decide se quer rever o material ou não.

Fale para seus alunos

É possível que outras pessoas acessem sua conta mesmo sem terem descoberto sua senha. Se alguém tiver informações pessoais suficientes sobre você, poderá tentar encontrar a senha com elas ou poderá convencer alguém em uma empresa a passar seus dados. Como essa pessoa não está usando tecnologia para invadir sua conta, esse tipo de ataque é chamado de hacking social ou engenharia social.

Pergunte aos seus alunos

Levante a mão se já esqueceu a senha de determinado site.

O que acontece quando você clica em “Esqueci minha senha”?

1. O site normalmente faz perguntas de segurança ou tenta entrar em contato com você por telefone ou email.

Quais são algumas das perguntas de segurança feitas pelo site?

1. Explique como algumas dessas perguntas podem ser respondidas ou adivinhadas por amigos ou conhecidos. Coisas como: nome do animal de estimação, local de nascimento, nome de solteira da mãe, nome do(a) professor(a) favorito(a), nome do(a) melhor amigo(a), time de futebol.

Quem mais pode saber esse tipo de informação sobre você?

Como um site entra em contato quando você esquece a senha?

Quem mais pode ter acesso a esses pontos de contato?

Pergunte aos seus alunos

Como um estranho pode descobrir as informações pessoais associadas às respostas das perguntas de segurança?

1. Publicações em redes sociais, pesquisas online de informações públicas, adivinhação, contato com seus amigos e outros.

Quais são alguns exemplos de publicações de redes sociais com informações pessoais?

1. Por exemplo, o Instagram de seu gato com o nome na legenda, uma foto com local marcado ou publicações de aniversário públicas.

Como você pode usar o Google para aprender mais sobre alguém e hackear sua senha?

1. Se um mecanismo de busca mostra a você a foto do 9º ano de alguém em um jornal de colégio online, é possível descobrir o nome do(a) professor(a).

Parte 2

Fale para seus alunos

É pouco seguro publicar informações que contenham respostas das perguntas de segurança. Escolha perguntas de segurança com respostas que só você sabe. Também é possível inventar respostas de perguntas de segurança, desde que você as salve em um gerenciador de senhas ou que sejam fáceis de guardar.

Alguns sites podem entrar em contato com os usuários pelo telefone ou por um email associado à conta. Se um usuário esquecer a senha, os sites costumam fornecer uma senha temporária ou um hiperlink para redefini-la.

Pergunte aos seus alunos

Essa é uma maneira segura de garantir que a pessoa que solicitou a nova senha é realmente o usuário?

E se você divulgou o endereço de email associado à conta?

1. O método de link de redefinição de senha é seguro na maioria das vezes, mas se a conta ou senha tiver sido divulgada para outras pessoa, você corre esse risco.

Fale para seus alunos

O hacking social também pode ser feito pelo contato direto de pessoas que tentam enganá-lo para que você forneça informações pessoais. Às vezes, pessoas

enviarão emails fingindo ser outra pessoa (como um amigo, um membro da família ou alguém do banco) e pedindo para você confirmar informações pessoais (como a data de nascimento) para verificar sua identidade. Isso também pode ser mais sutil, por exemplo, se alguém invadir a conta de rede social de um amigo seu e enviar mensagem para você (e possivelmente para outras pessoas) perguntando sobre seu aniversário ou cidade natal. Se você receber mensagens de amigos que parecem estranhas, tente entrar em contato com eles (fora da plataforma de rede social) a fim de descobrir se eles realmente enviaram esse conteúdo.

Ataques que usam emails ou sites com aparência real são chamados de phishing (fraude eletrônica) e podem levar a roubo de identidade. Por exemplo, um ladrão de identidade pode abrir cartões de crédito em seu nome e usá-los, o que poderá dificultar abrir novos cartões de crédito quando você for mais velho.

Phishing pode permitir que o ladrão se passe por você e acesse outras informações, ganhando acesso a emails, mandando mensagens para seus amigos como se fosse você ou roubando seu dinheiro. Esse processo também pode permitir que o ladrão te bloqueie em sua conta criando uma nova senha que você não conhece.

Tarefa

Folheto

Atribuição

Peça aos participantes que respondam às perguntas a seguir e adicionem as respostas em texto ou imagem no folheto sobre senhas.

1. Quais são as três informações obtidas nesta lição que você aplicará da próxima vez que tiver que criar uma senha?

2. Indique uma situação em que você acha que não há problemas em compartilhar sua senha com alguém.

3. Quais são as três estratégias que você pode usar para compartilhar uma senha com alguém de forma segura?

4. Dê três exemplos do que pode dar errado se a senha cair em mãos erradas?