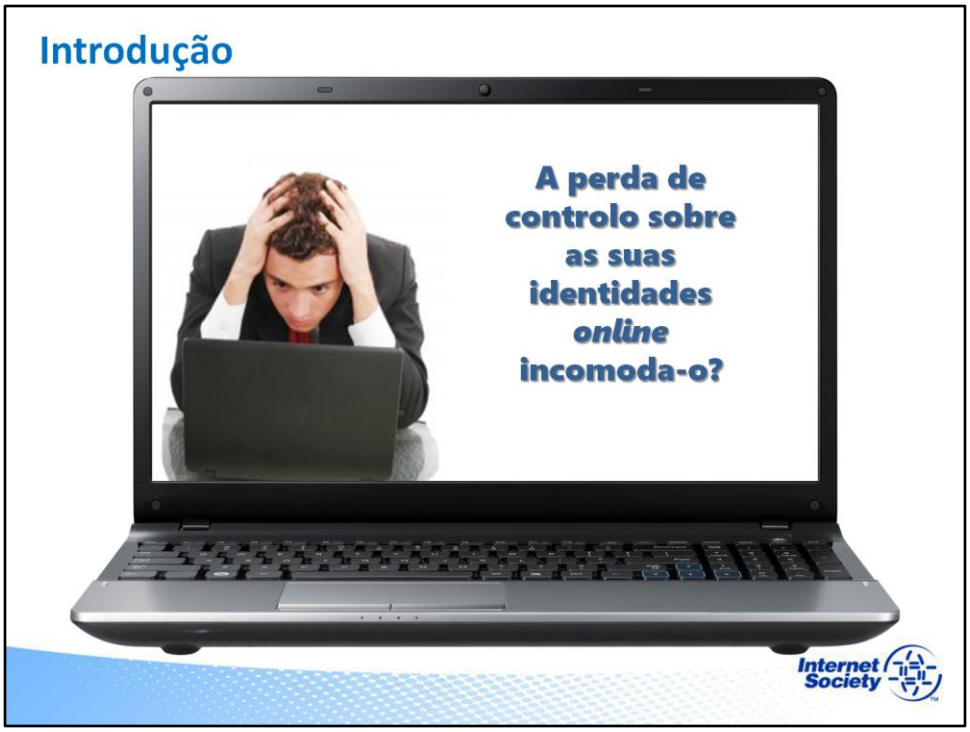
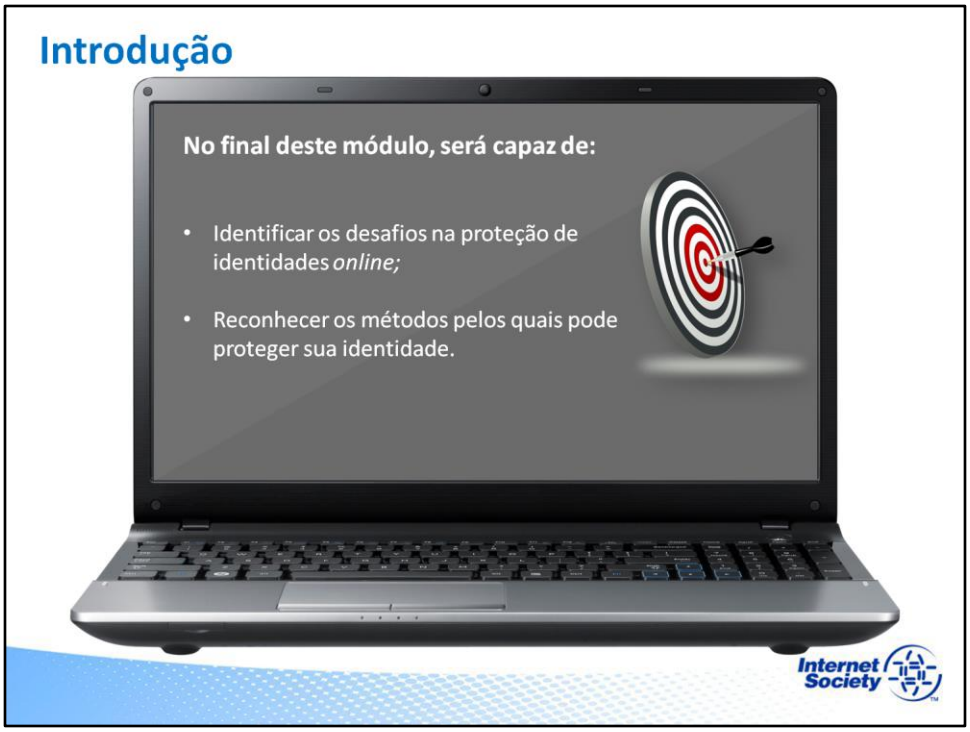
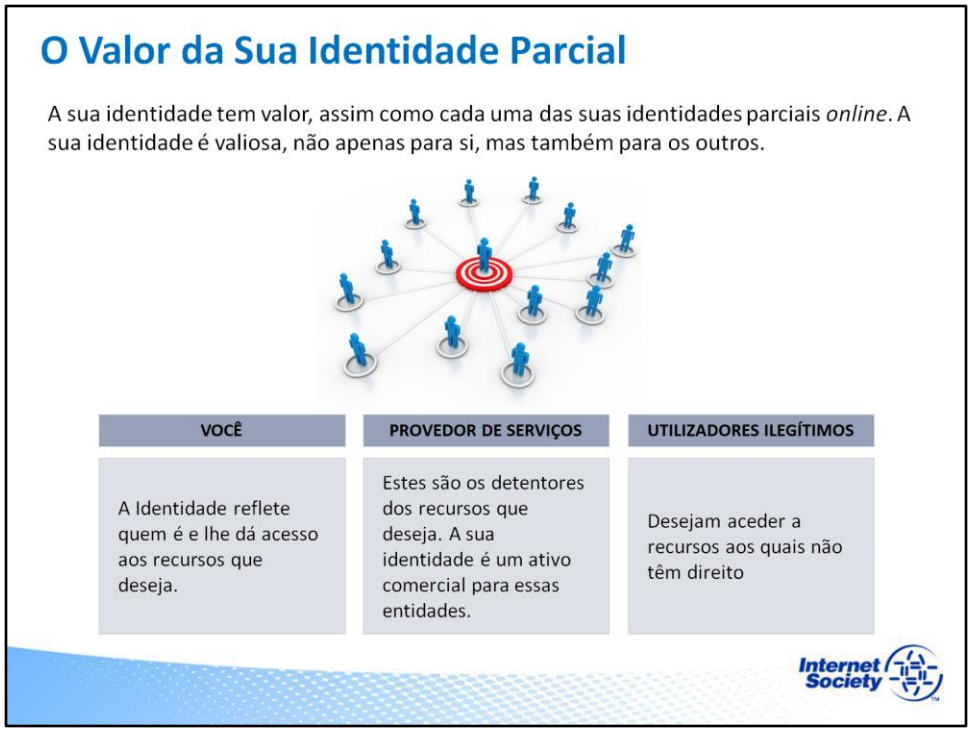
Bem-vindo a Gestão da Identidade - módulo 3, onde aprenderemos a proteger a sua identidade



A perda de controlo sobre as suas identidades *online* incomoda-o? Se não, talvez deva reconsiderar.
Isto pode ser motivo de preocupação para qualquer utilizador ativo da Internet.



No final deste módulo, será capaz de:
• Identificar os desafios na proteção de identidades *online*
• Reconhecer os métodos pelos quais pode proteger sua identidade



A sua identidade tem valor, assim como cada uma das suas identidades parciais *online*. A sua identidade é valiosa, não apenas para si, mas também para os outros. Tem valor para si enquanto indivíduo, porque sua identidade reflete quem é e lhe dá acesso aos recursos que deseja.

Segundo, tem valor para o provedor de serviços que confia na sua afirmação de identidade, por exemplo, o banco ou um site de redes sociais, como o Facebook ou o Twitter. Estes são os detentores dos recursos que deseja. A sua identidade é um ativo comercial para essas entidades. Quando a sua identidade parcial está no seu banco ou numa corretora, esta pode ter um valor monetário direto. Quando se trata de um site de redes sociais, o valor pode ser menos tangível, mas igualmente importante para si.

Por fim, sua identidade é valiosa para os ladrões e outros utilizadores ilegítimos da sua identidade que desejam aceder a recursos aos quais não têm direito. À medida que o valor das suas identidades parciais aumenta, os seus dados tornam-se cada vez mais atraentes para os ladrões.

O que é Furto de Identidade?

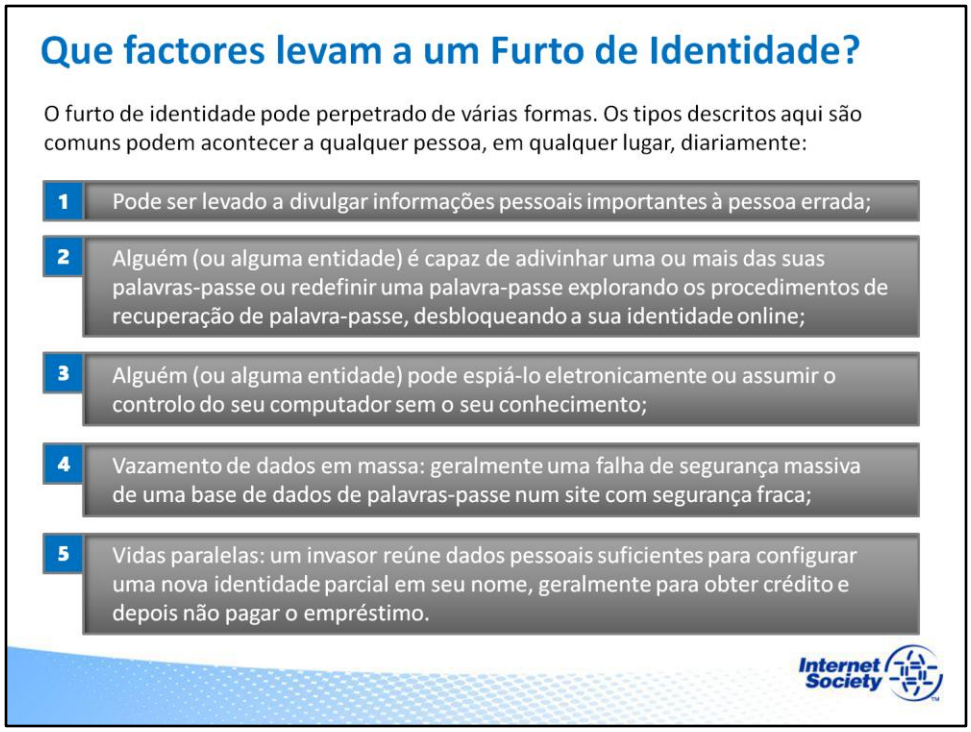
O furto de identidade, geralmente entende-se pela perda de controlo sobre uma ou mais de suas identidades parciais.

Sendo que quaisquer identidades parciais online podem conter dados particulares, é importante fazer a sua gestão e protegê-las adequadamente.

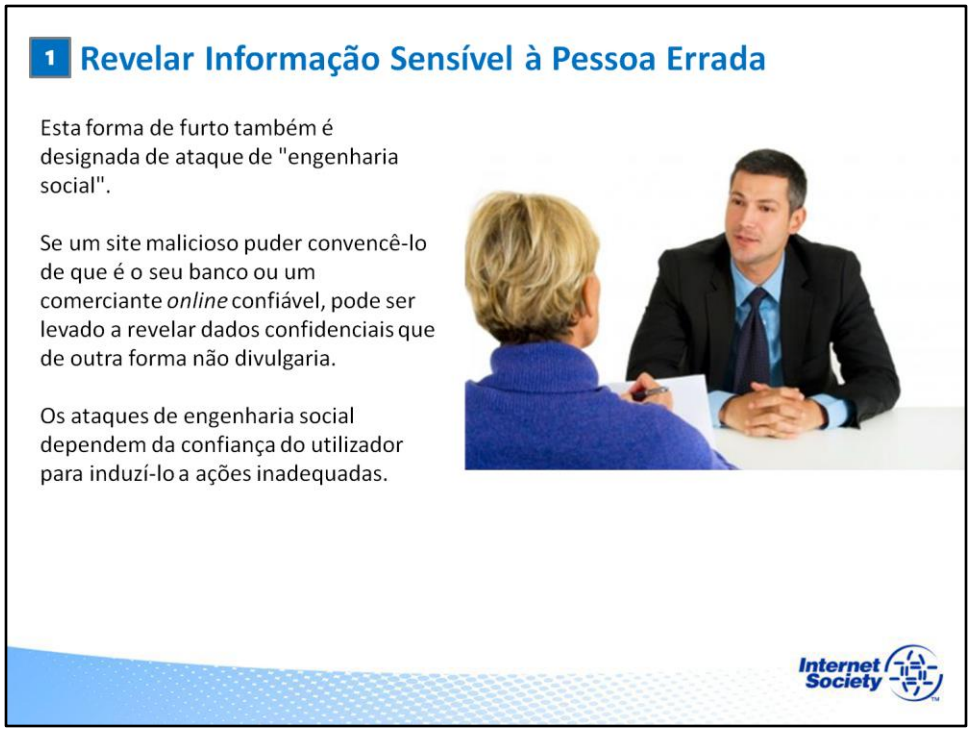
A maioria dos furtosde identidade são uma etapa no processo da fraude de identidade; refletindo o valor monetário direto de algumas identidades parciais.

Internet Society

O furto de identidade, geralmente entende-se pela perda de controlo sobre uma ou mais de suas identidades parciais.
Sendo que quaisquer identidades parciais online podem conter dados particulares, é importante fazer a sua gestão e protegê-las adequadamente.
A maioria dos furtos de identidade são uma etapa no processo da fraude de identidade; refletindo o valor monetário direto de algumas identidades parciais.

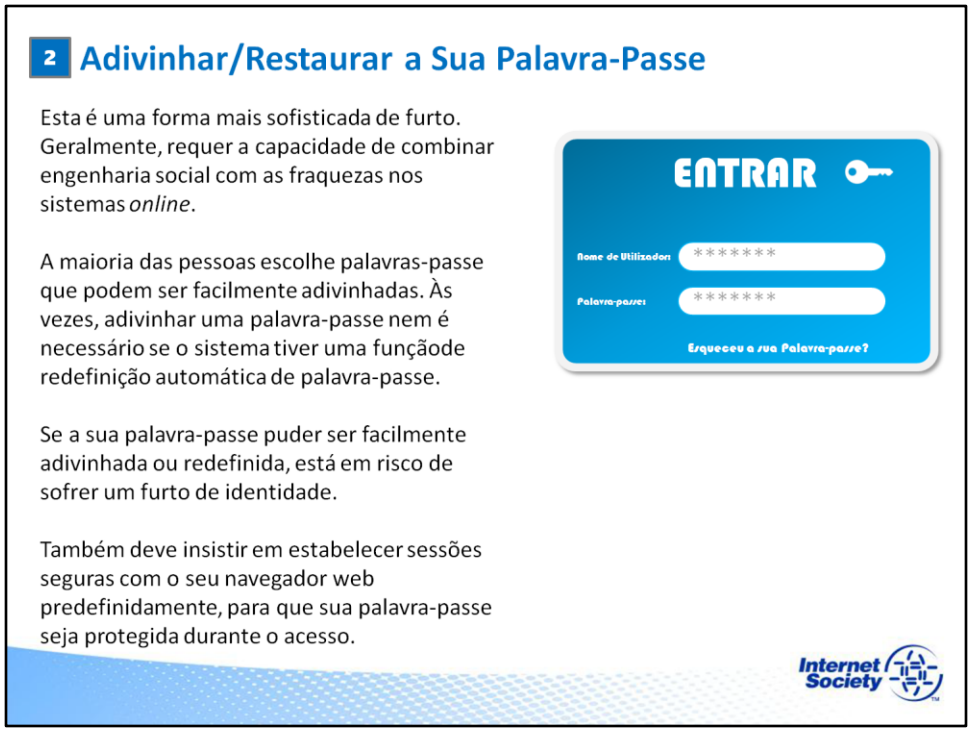


O furto de identidade pode ser perpetrado de várias formas. Os tipos descritos aqui são comuns podem acontecer a qualquer pessoa, em qualquer lugar, diariamente:
1.Pode ser levado a divulgar informações pessoais importantes à pessoa errada;
2.Alguém (ou alguma entidade) é capaz de adivinhar uma ou mais das suas palavras-passe ou redefinir uma palavra-passe explorando os procedimentos de recuperação desta, desbloqueando a sua identidade *online*;
3. Alguém (ou alguma entidade) pode espiá-lo eletronicamente ou assumir o controlo do seu computador sem o seu conhecimento;
4. Vazamento de dados em massa: geralmente o *hacking* ou a aquisição de um arquivo completo de bases de dados de terceiros com fragilidades de segurança. Já sucedeu por várias ocasiões, por exemplo, em lojas *online* e em sistemas de jogos *online*;
5.Vidas paralelas quando um invasor reúne dados pessoais suficientes para configurar uma nova identidade parcial em seu nome, geralmente para obter crédito e depois não pagar o empréstimo.
Vamos aprender sobre cada um desses tipos de furto.



Esta forma de furto também é designada de ataque de "engenharia social". Se um site malicioso puder convencê-lo de que é o seu banco ou um comerciante *online* confiável, pode ser levado a revelar dados confidenciais que de outra forma não divulgaria. Os ataques de engenharia social dependem da confiança do utilizador para induzí-lo a ações inadequadas.

Uma parte considerável do e-mail não solicitado ou "spam" enviado aos utilizadores da Internet é projetada para roubar informações pessoais.
Essas mensagens de "phishing" tentam convencê-lo a visitar um site malicioso criado para roubar a sua identidade ou divulgar outros dados, como detalhes de pagamento, na crença equivocada de que está a lidar com um site confiável.



Esta é uma forma mais sofisticada de furto. Geralmente, requer a capacidade de combinar engenharia social com as fraquezas nos sistemas *online*. Infelizmente, a maioria das pessoas escolhe palavras-passe que, com um pouco de reflexão e paciência, podem ser facilmente adivinhadas. Às vezes, adivinhar uma palavra-passe nem é necessário se o sistema tiver uma função de redefinição automática de palavra-passe. De facto, muitos sistemas *online* permitem que qualquer pessoa redefina uma palavra-passe, desde que sejam conhecidos alguns factos sobre o titular da conta.

Se a sua palavra-passe puder ser facilmente adivinhada ou redefinida, está em risco de sofrer um furto de identidade.

Também deve insistir em estabelecer sessões seguras com o seu navegador web predefinidamente, para que sua palavra-passe seja protegida durante o acesso.

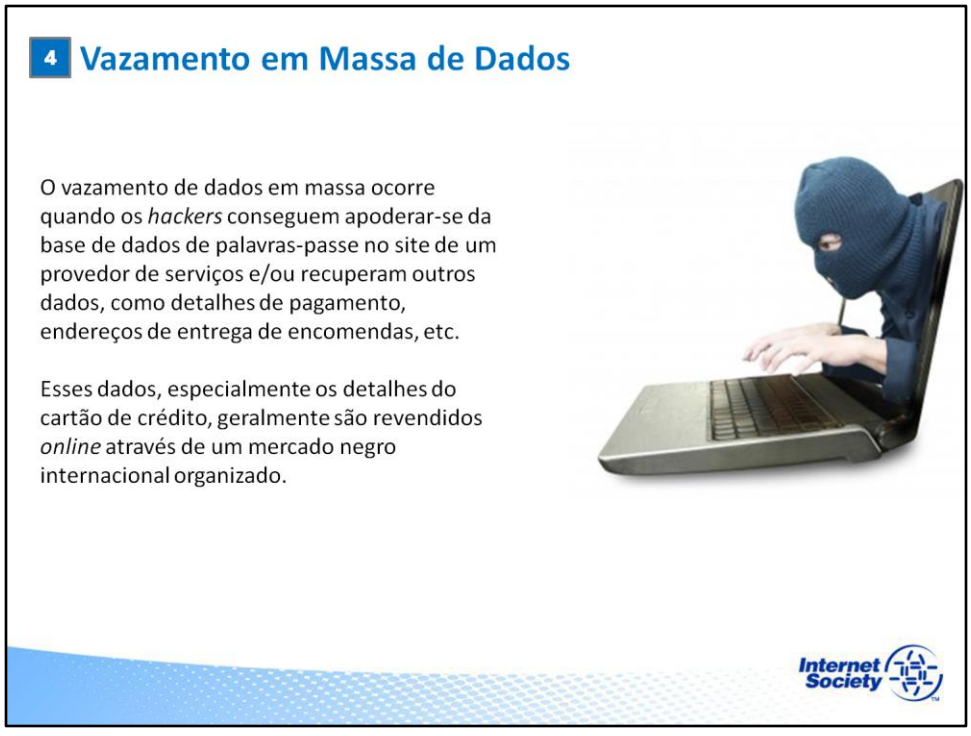
3 Escutá-lo Electronicamente

Essa é uma forma de furto mais sofisticada do ponto de vista tecnológico.

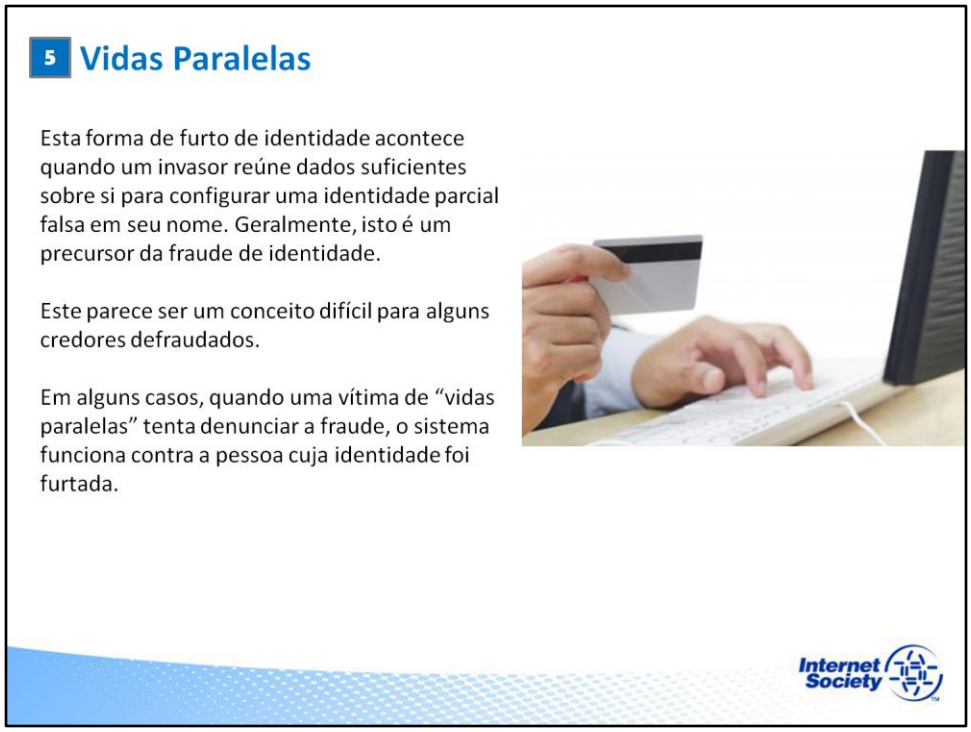
Geralmente depende de malware (como um vírus) que assume o controlo de um computador ou de uma rede de computadores e, em seguida, procura informações confidenciais, como números de cartão de crédito, nomes de utilizador e palavras-passe online, etc.

Internet Society

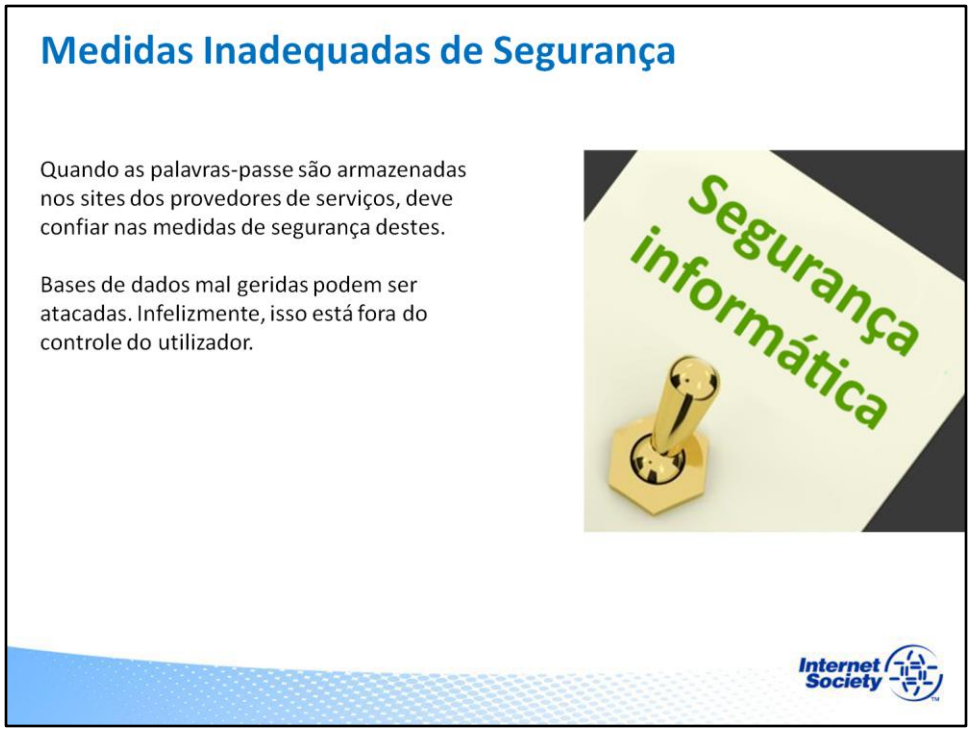
Esta é uma forma de furto mais sofisticada do ponto de vista tecnológico. Geralmente depende de malware (como um vírus) que assume o controlo de um computador ou de uma rede de computadores e, em seguida, procura informações confidenciais, como números de cartão de crédito, nomes de utilizador e palavras-passe online, etc.



O vazamento de dados em massa ocorre quando os *hackers* conseguem apoderar-se da base de dados de palavras-passe no site de um provedor de serviços e/ou recuperam outros dados, como detalhes de pagamento, endereços de entrega de encomendas, etc.
Esses dados, especialmente os detalhes do cartão de crédito, geralmente são revendidos *online* através de um mercado negro internacional organizado.



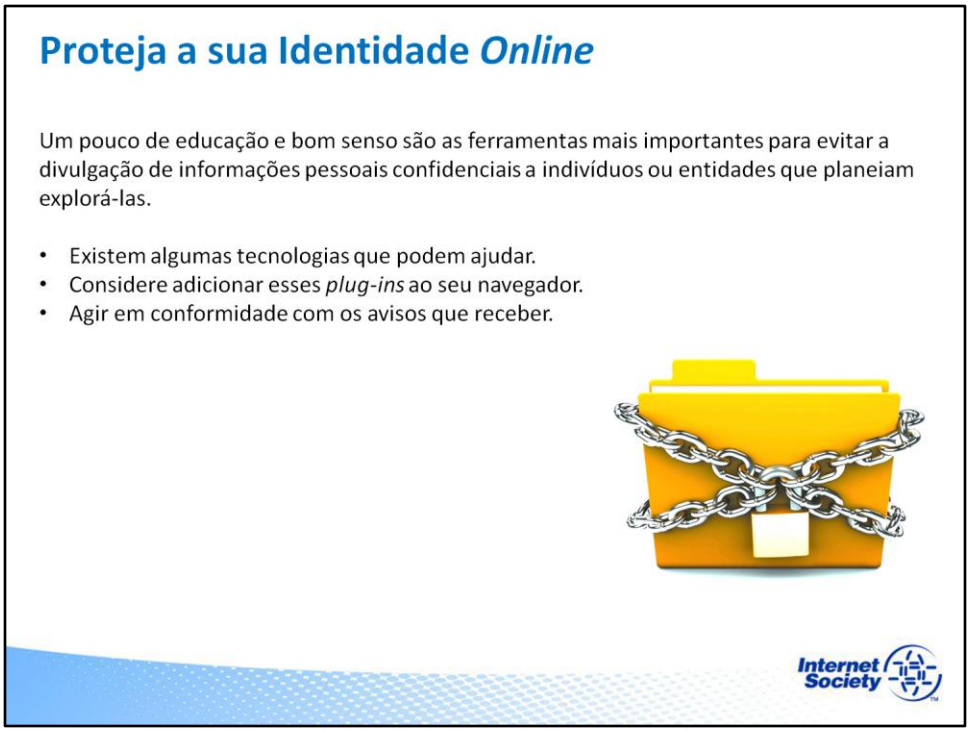
Esta forma de furto de identidade acontece quando um invasor reúne dados suficientes sobre si para configurar uma identidade parcial falsa em seu nome. Geralmente, isto é um precursor da fraude de identidade: o invasor usa os seus dados pessoais para solicitar crédito e, em seguida, deixa-o com a dívida. A primeira vez que souber disso, pode ser quando o credor começa a contactá-lo para fazer a cobrança. Quando uma vítima de "vidas paralelas" informa o credor da fraude, a resposta do credor geralmente é "Como assim? Então, você não é o Sr. Silva?"
"Sim, sou o Sr. Silva, mas a pessoa que fez esse empréstimo não era eu."
Este parece ser um conceito difícil para alguns credores defraudados.
Em alguns casos, quando uma vítima de "vidas paralelas" tenta denunciar a fraude, a polícia diz que não pode registar uma ocorrência com base no relatório da vítima, porque, de acordo com a lei, o credor é a verdadeira vítima e a polícia não pode fazer nada, a não ser que o credor formalize uma reclamação.
Portanto, o sistema funciona contra a pessoa cuja identidade foi furtada.



No entanto, o furto de identidade por meio de escutas e vazamento de dados em massa às vezes é possível devido à segurança inadequada por parte do fornecedor de serviços. Quando as palavras-passe são armazenadas nos sites dos fornecedores de serviços, deve confiar nas medidas de segurança destes e no nível de responsabilidade que estão preparados para acionar em caso de falhas na segurança. Na pior das hipóteses, os fornecedores de serviços transmitem ou armazenam palavras-passe (e até detalhes do cartão de crédito) nos seus sistemas.

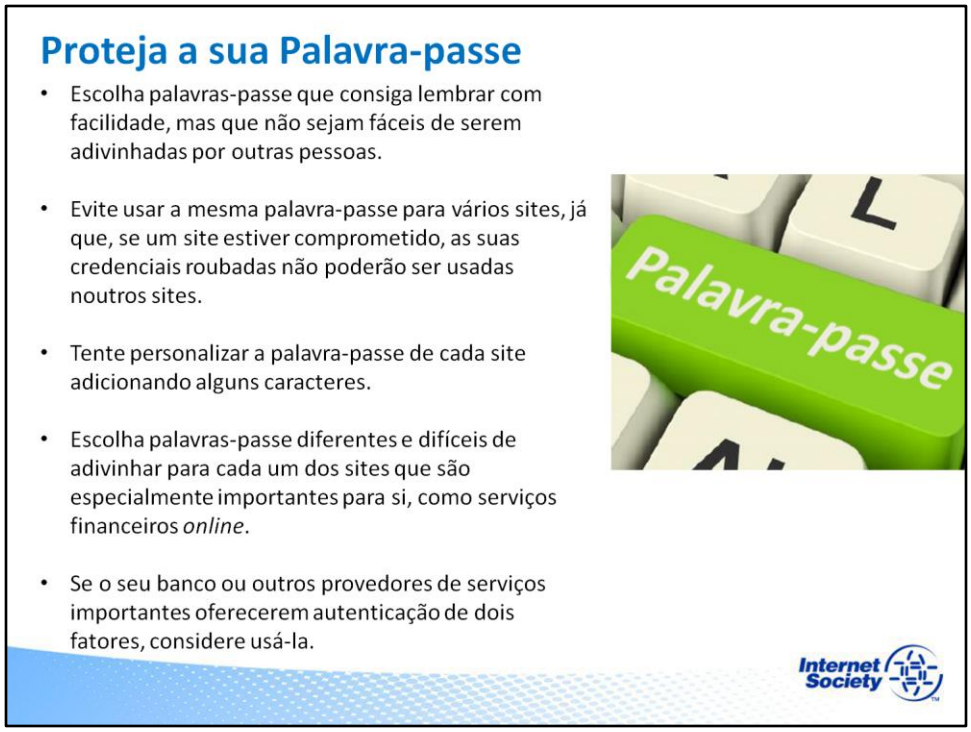
Bases de dados mal geridas podem ser atacadas. Infelizmente, isso está fora do controle do utilizador, mas cada vez que um fornecedor de serviços sofre uma brecha de dados embaraçosa (ou ação judicial) neste âmbito, isso aumenta a pressão sobre outros no sentido adotarem boas práticas.

Realmente não tem muito controle direto nesta questão além da sua capacidade em mudar de provedor de serviços e, às vezes, essa escolha pode não suscitar grande diferença. Se uma empresa extraviar os seus dados pessoais, é provável que o seu acesso a representação jurídica dependa da jursidição em que se encontra e mediante a sua capacidade de provar os danos que sofreu em resultado disto.



Um pouco de educação e bom senso são as ferramentas mais importantes para evitar a divulgação de informações pessoais confidenciais a indivíduos ou entidades que planeiam explorá-las.

Existem algumas tecnologias que podem ajudar. As versões mais recentes da maioria dos navegadores Web têm a capacidade de verificar sites e alertá-lo sobre sites maliciosos. Considere adicionar esses *plug-ins* ao seu navegador, mas lembre-se que a sua proteção não é assegurada só por adicionar um *plug-in*: tem que agir em conformidade com os avisos que receber, caso contrário, não estará mais seguro do que antes. Inicialmente, pode achar as mensagens de aviso inconvenientes - mas use-as como uma forma de se habituar às práticas de segurança. Vai valer a pena a longo prazo.



Vamos aprender agora sobre algumas das maneiras pelas quais pode proteger sua identidade.

Proteja a sua palavra-passe. Se uma palavra-passe é fácil de adivinhar, é fácil roubá-la. Escolha palavras-passe que consiga lembrar com facilidade, mas que não sejam fáceis de serem adivinhadas por outras pessoas.

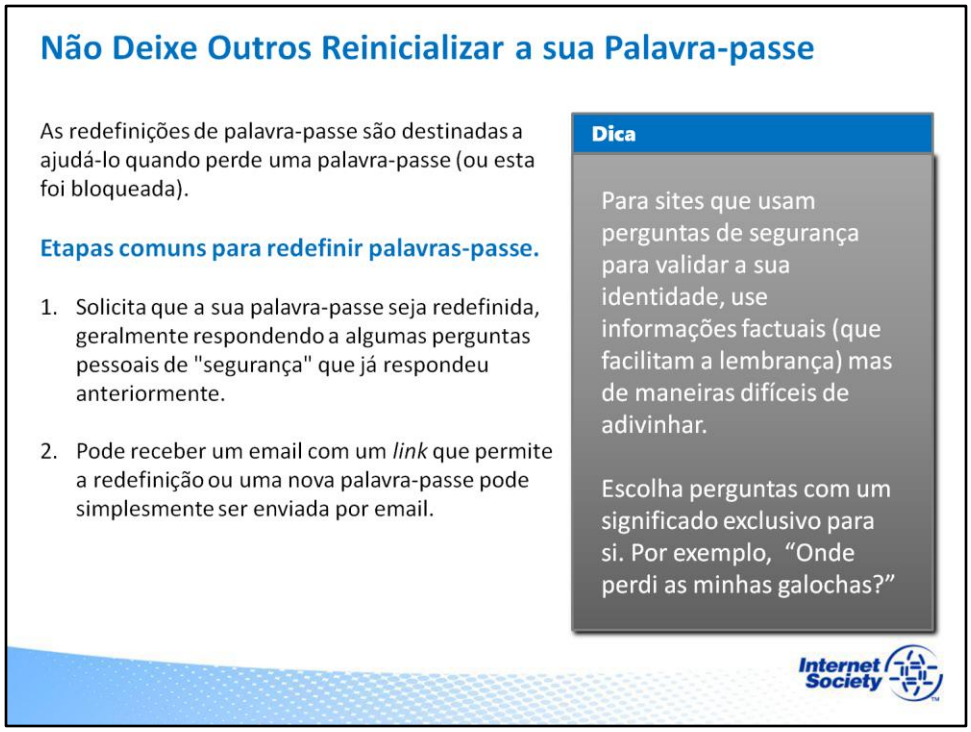
Evite usar a mesma palavra-passe para vários sites, já que, se um site estiver comprometido, as suas credenciais roubadas não poderão ser usadas noutros sites.

Se deseja selecionar palavras-passe relacionadas para facilitar a lembrança, tente personalizar a palavra-passe de cada site adicionando alguns caracteres (como o nome do site). Isto não engana um invasor dedicado, mas impede qualquer um que tente usar a sua palavra-passe em outros sites. O princípio crucial aqui é manter o pragmatismo, protegendo contra os ataques mais prováveis.

Seja especialmente cuidadoso ao escolher palavras-passe diferentes e difíceis de adivinhar para cada um dos sites que são realmente importantes para si, como serviços financeiros *online*. Muitos sites, particularmente aqueles que mantêm informações financeiras ou de saúde, empregam várias técnicas para impedir que os ladrões tentem entrar na sua conta. Uma defesa bloqueia automaticamente uma conta quando detecta falhas repetidas de autenticação, o que pode indicar que alguém está a tentar adivinhar a sua palavra-passe.

Se o seu banco ou outros provedores de serviços importantes oferecerem autenticação de dois fatores, considere usá-la, a menos que o seu banco concorde em assumir toda a responsabilidade caso sua palavra-passe seja comprometida.

Vamos aprender mais sobre isto.



As redefinições de palavra-passe são destinadas a ajudá-lo quando perde uma palavra-passe (ou esta foi bloqueada). Todos os sites têm uma técnica ligeiramente diferente para redefinir uma palavra-passe. Aqui estão as etapas mais comuns para redefinir palavras-passe.

1.Solicita que a sua palavra-passe seja redefinida, geralmente respondendo a algumas perguntas pessoais de "segurança" que já respondeu anteriormente.

2.Pode receber um email com um *link* que permite a redefinição ou uma nova palavra-passe pode simplesmente ser enviada por email. Para sites que usam perguntas de segurança para validar a sua identidade, use informações factuais (que facilitam a lembrança) mas de maneiras difíceis de adivinhar. Por exemplo, se a pergunta solicitar o nome da primeira escola que frequentou ou o nome da primeira rua em que viveu, responda com a segunda escola que frequentou ou a segunda rua em que morou. Dessa forma, mesmo alguém que sabe muito sobre si terá dificuldade em responder às perguntas. Além disso, lembre-se que não precisa de fornecer respostas "lógicas", desde que estas façam sentido para si e sejam fáceis de memorizar. Por exemplo, se a pergunta de segurança perguntar "Qual é a sua cor favorita", não existem obstáculos a que indique simplesmente "três" ou "olhos de Monica" como resposta e será muito mais difícil para um invasor adivinhar isto.

Proteja o Acesso ao seu Email

Com redefinições de palavra-passe, é importante que proteja o seu email, pois o seu endereço de email geralmente é vital ao processo de redefinição.

Qualquer pessoa que tenha acesso ao seu email poderá redefinir as suas palavras-passe e obter acesso às suas contas.

A proteção do acesso ao seu email é uma das ferramentas mais importantes para proteger a sua identidade *online*.

Particularmente, se sua conta de e-mail principal oferecer autenticação de dois fatores, vale a pena considerar a camada extra de proteção para esse ativo confidencial.

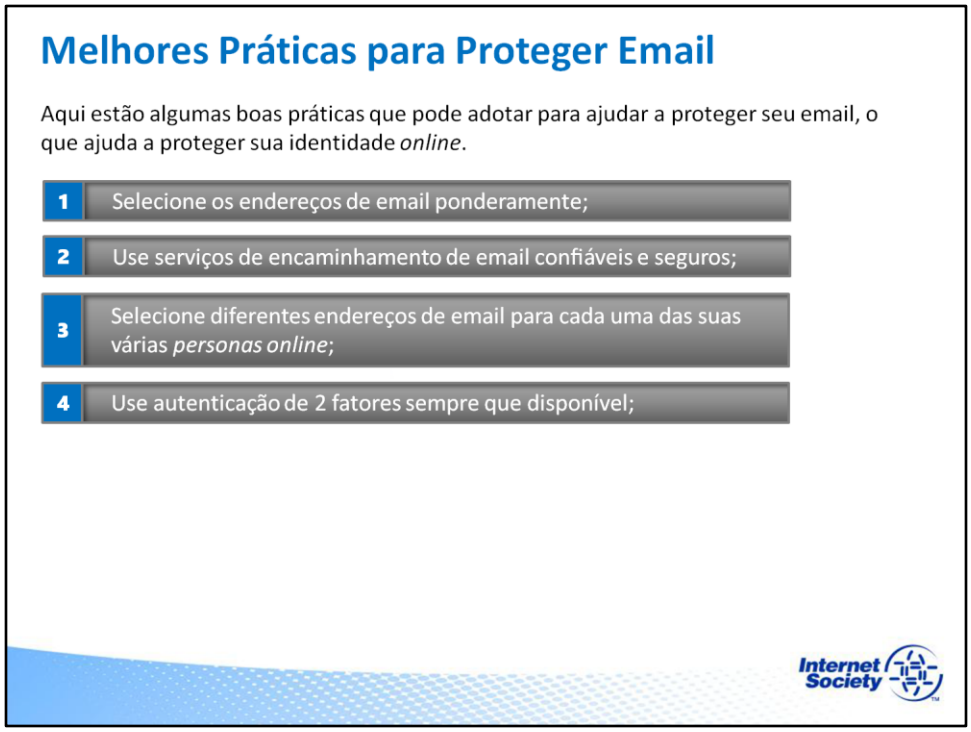
Internet Society

Com redefinições de palavra-passe, é importante que proteja o seu email, pois o seu endereço de email geralmente é vital ao processo de redefinição; ou seja, qualquer pessoa que tenha acesso ao seu email poderá redefinir as suas palavras-passe e obter acesso às suas contas. A proteção do acesso ao seu email é uma das ferramentas mais importantes para proteger a sua identidade *online*.
Particularmente, se sua conta de e-mail principal oferecer autenticação de dois fatores, vale a pena considerar a camada extra de proteção para esse ativo confidencial.

As três técnicas comuns adotadas pela maioria dos utilizadores da Internet para se protegerem online são:

- Sair das contas quando terminar a sessão;
- Usar protocolos encriptados (https ou email protegido por SSL);
- Alterar palavras-passe periodicamente.

Alguns serviços de e-mail (por exemplo, fastmail.fm) também oferecem a opção de múltiplas palavras-passe: uma palavra-passe pode ser para uso em ambientes suspeitos. Esta fornece acesso ao seu e-mail, mas não permite excluir e-mails, editar pastas ou alterar as configurações da sua conta.



Aqui estão algumas boas práticas que pode adotar para ajudar a proteger seu email, o que ajuda a proteger sua identidade *online*.

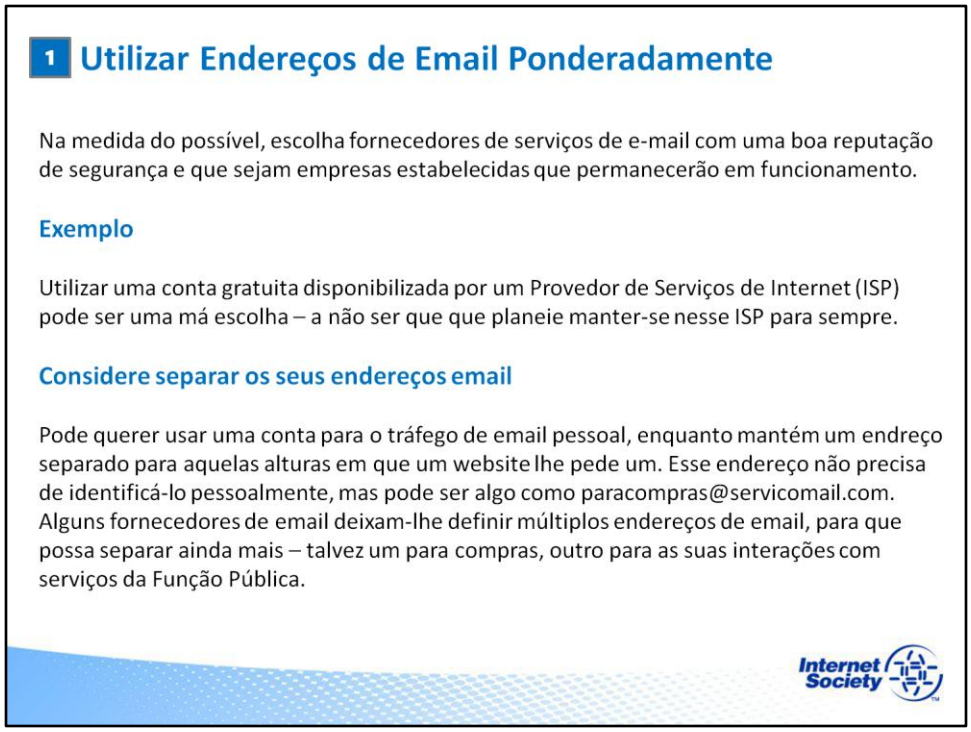
1.Selecione os endereços de email ponderamente;

2.Use serviços de encaminhamento de email confiáveis e seguros;

3. Selecione diferentes endereços de email para cada uma das suas várias *personas online*;

4.Use autenticação de 2 fatores sempre que lhe é disponibilizada a opção.

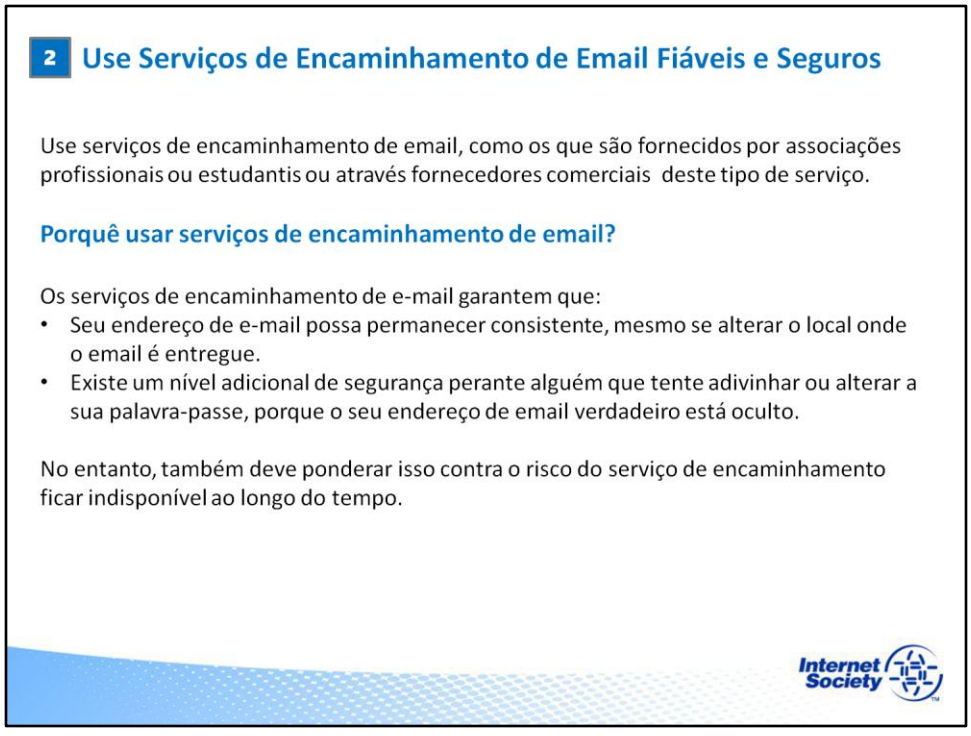
Vamos aprender mais sobre essas técnicas e porque é aconselhável aplicá-las.



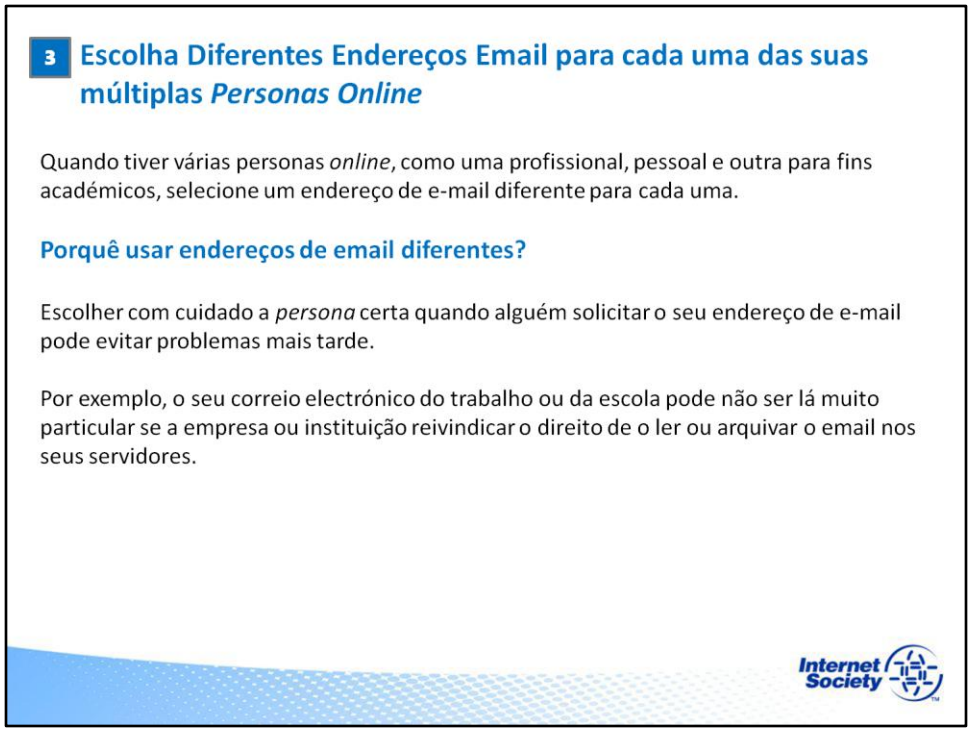
Na medida do possível, escolha fornecedores de serviços de e-mail com uma boa reputação de segurança e que sejam empresas estabelecidas que provavelmente permanecerão em funcionamento: por mais improvável que pareça, dedique alguns minutos para pensar em como pode mitigar o risco de um de seus fornecedores de e-mail desaparecer de um momento para o outro.

A Internet não vai desaparecer tão cedo, por isso deseja criar contas de e-mail que poderá usar durante as próximas décadas. Um único endereço de email principal facilitará a redefinição de palavras-passe esquecidas e reduzirá a probabilidade de alguém roubar a sua identidade iniciando sessão numa conta esquecida. No entanto, lembre-se do princípio estabelecido pela lenda viva do investimento, Warren Buffett: "Pode ser boa idea colocar todos os seus ovos numa cesta, desde que cuide muito bem dessa cesta".

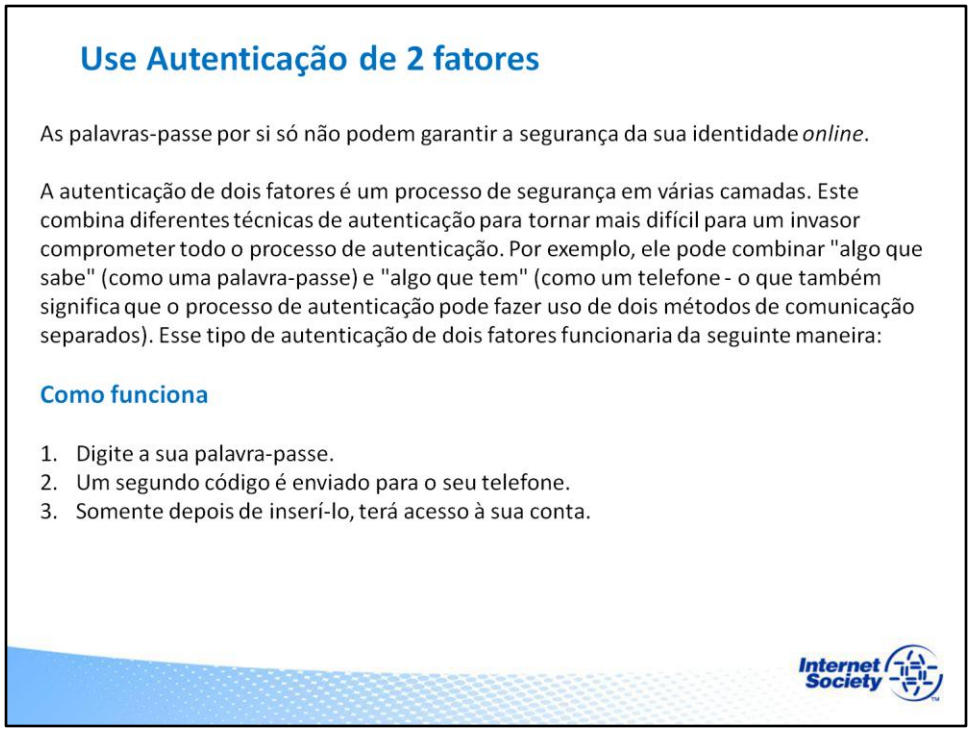
Se possui o seu próprio domínio, pode até criar um endereço de e-mail diferente para cada site que solicite esse elemento. Desta forma, pode fornecer ao Google o endereço google@omeudominio.com e à Amazon o endereço amazon@omeudominio.com . Além de limitar a possibilidade do invasor comprometer sua conta de e-mail pessoal, essa abordagem facilita a identificação do momento em que estes provedores de serviços estão a partilhar o seu endereço de email com terceiros, já que se tornará óbvio quando começar a receber emails endereçados ao amazon@omeudominio.com cujo remetente não é a Amazon.



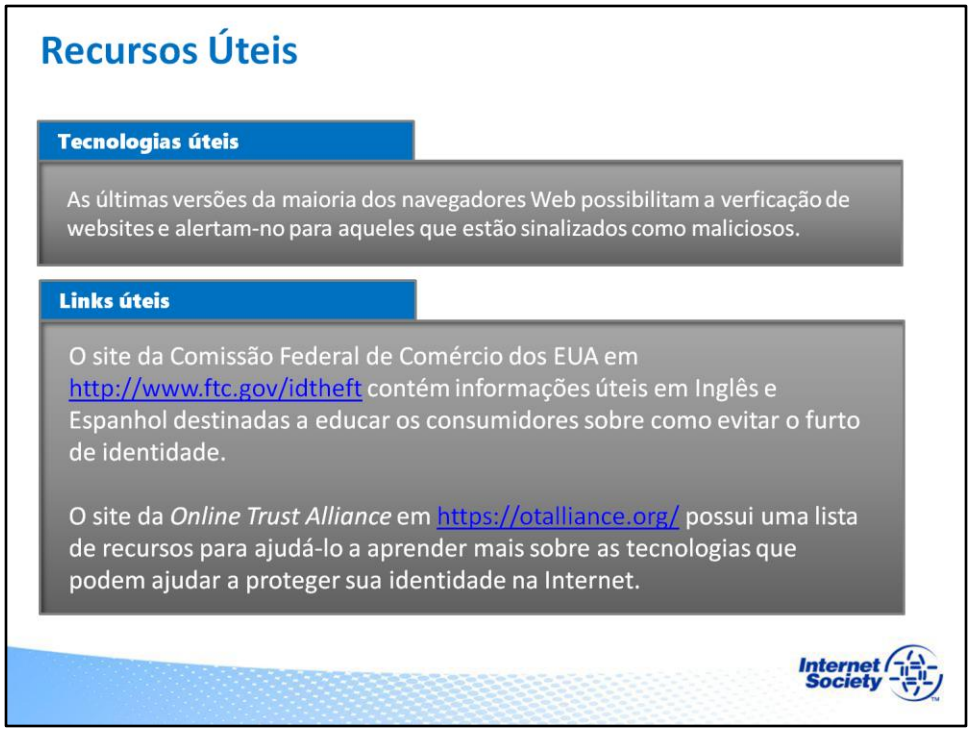
Use serviços de encaminhamento de email, como os que são fornecidos por associações profissionais ou estudantis ou através fornecedores comerciais deste tipo de serviço.
Porquê usar serviços de encaminhamento de email?
Os serviços de encaminhamento de e-mail garantem que o seu endereço de e-mail possa permanecer consistente, mesmo se alterar o local onde o email é entregue. Além disso, passa a existir um nível adicional de segurança perante alguém que tente adivinhar ou alterar a sua palavra-passe, porque o seu endereço de email verdadeiro está oculto. No entanto, também deve ponderar isso contra o risco do serviço de encaminhamento ficar indisponível ao longo do tempo.



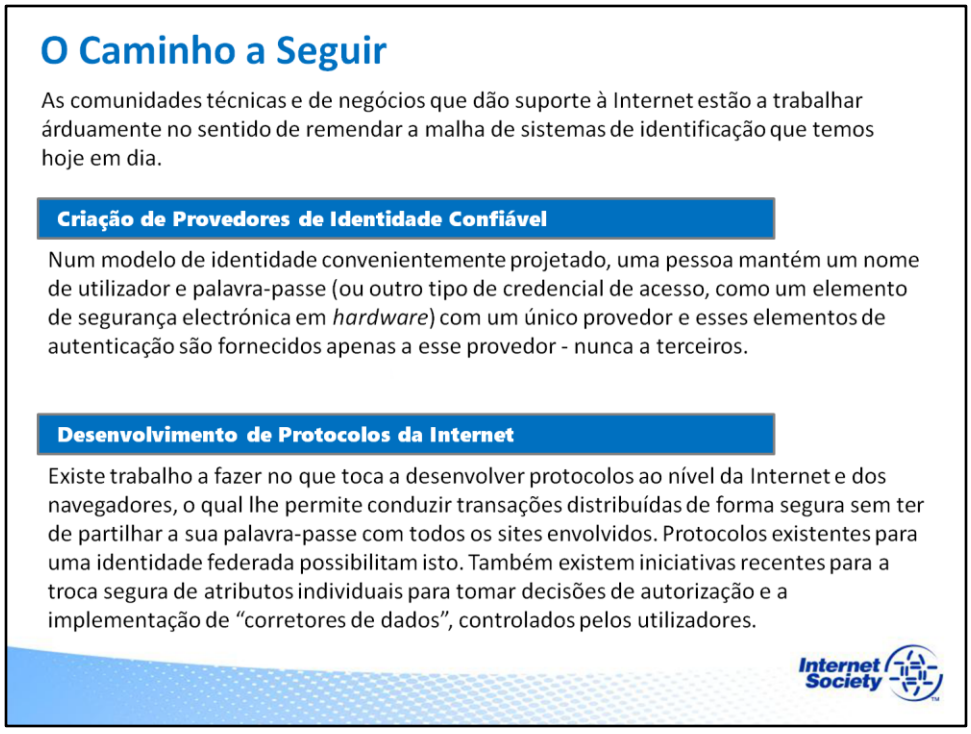
Quando tiver várias personas *online*, como uma profissional, pessoal e outra para fins académicos, selecione um endereço de e-mail diferente para cada uma.
Porquê usar endereços de email diferentes?
Escolher com cuidado a *persona* certa quando alguém solicitar o seu endereço de e-mail pode evitar problemas mais tarde.
Por exemplo, o seu correio electrónico do trabalho ou da escola pode não ser lá muito particular se a empresa ou instituição reivindicar o direito de o ler ou arquivar o email nos seus servidores.



As palavras-passe por si só não podem garantir a segurança da sua identidade *online*. Se alguém tiver acesso à sua palavra-passe, poderá aceder facilmente à sua conta: o uso da autenticação de dois fatores pode tornar isto muito mais difícil.
A autenticação de dois fatores é um processo de segurança em várias camadas. Este combina diferentes técnicas de autenticação para tornar mais difícil para um invasor comprometer todo o processo de autenticação. Por exemplo, ele pode combinar "algo que sabe" (como uma palavra-passe) e "algo que tem" (como um telefone - o que também significa que o processo de autenticação pode fazer uso de dois métodos de comunicação separados). Esse tipo de autenticação de dois fatores funcionaria da seguinte maneira: primeiro digita a sua palavra-passe. Um segundo código é enviado para o seu telefone. Somente depois de inserí-lo, terá acesso à sua conta. Para subverter o processo de autenticação, um invasor agora precisa de saber, não só a sua palavra-passe, como também terá de interceptar uma mensagem separada, em tempo real, enviada para o seu telefone.
Embora nem todos os serviços ofereçam autenticação de dois fatores, um número crescente de fornecedores de serviços bancários e de e-mail disponibiliza isto e vale a pena adicionar essa camada extra de proteção, quando existe esta opção.



Para saber mais sobre o furto de identidade e como evitá-lo, visite os seguintes sites.
O site da Comissão Federal de Comércio dos EUA (http://www.ftc.gov/idtheft) contém informações úteis em inglês e espanhol destinadas a educar os consumidores sobre como evitar o furto de identidade.
O site da *Online Trust Alliance* em https://otalliance.org/ possui uma lista de recursos para ajudá-lo a aprender mais sobre as tecnologias que podem ajudar a proteger sua identidade na Internet.



As comunidades técnicas e de negócios que dão suporte à Internet estão a trabalhar árduamente para manter a autenticação e a autorização ao ritmo da evolução da utilização da Internet. Em particular, a autenticação e a autorização, na Internet de hoje, têm maior probabilidade de serem funções 'distribuídas' envolvendo mais de um provedor de serviços, sendo que antes disso, existiam de forma isolada. Muitas soluções para isto ainda estão em desenvolvimento.

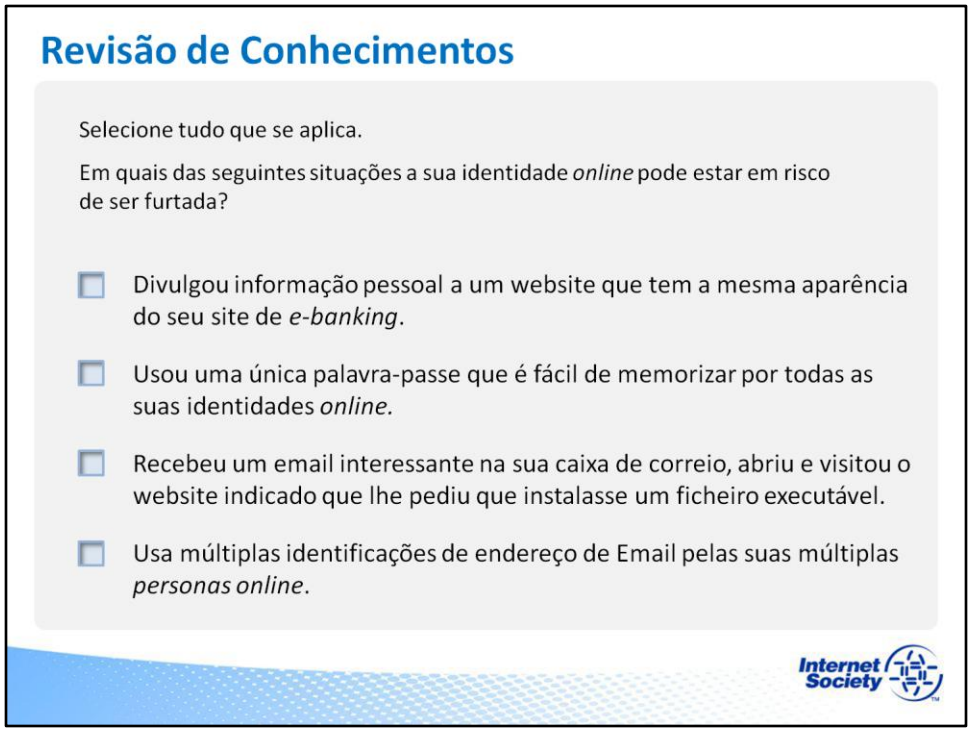
O modelo para o qual avançamos gradualmente envolve a criação de provedores de identidade confiáveis, certificados e com níveis reconhecíveis de segurança, bem como o aumento da dependência de terceiros para afirmar um único atributo de um utilizador, em vez de trocar detalhes de autenticação ou um perfil de utilizador inteiro. Isso significa, por exemplo, que uma entidade confiável pode simplesmente ter certeza de que você tem mais de 18 anos, sem precisar de conhecer todo o seu perfil pessoal.

Num modelo de identidade convenientemente projetado, uma pessoa mantém um nome de utilizador e palavra-passe (ou outro tipo de credencial de acesso, como um elemento de segurança electrónica em *hardware*) com um único provedor e esses elementos de autenticação são fornecidos apenas a esse provedor - nunca a terceiros.

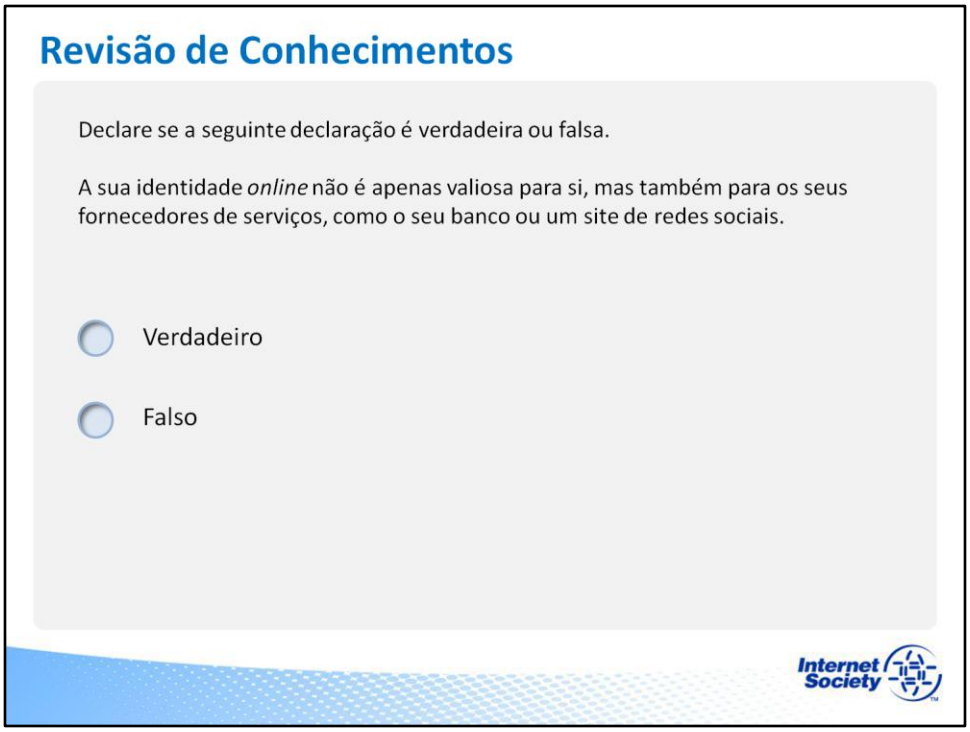
Os protocolos de identidade federada permitem que se autentique com segurança num site e receba serviços de outro, sem precisar de partilhar a sua palavra-passe ou informações privadas com este.

Essas tecnologias ficarão invisíveis para si, mas melhorarão a segurança, operando

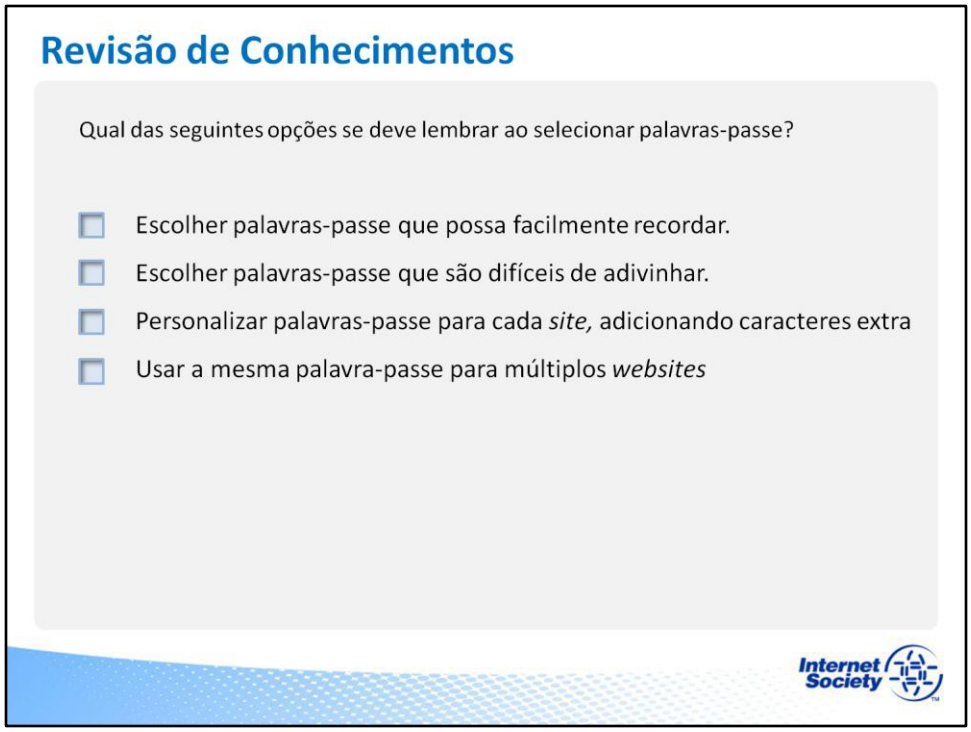
para manter sua identidade segura. As abordagens mais recentes envolvem processos através dos quais o utilizador mantém mais controlo sobre o fluxo de informações para os fornecedores de serviços, por meio de "corretores de dados", controlados pelos utilizadores.



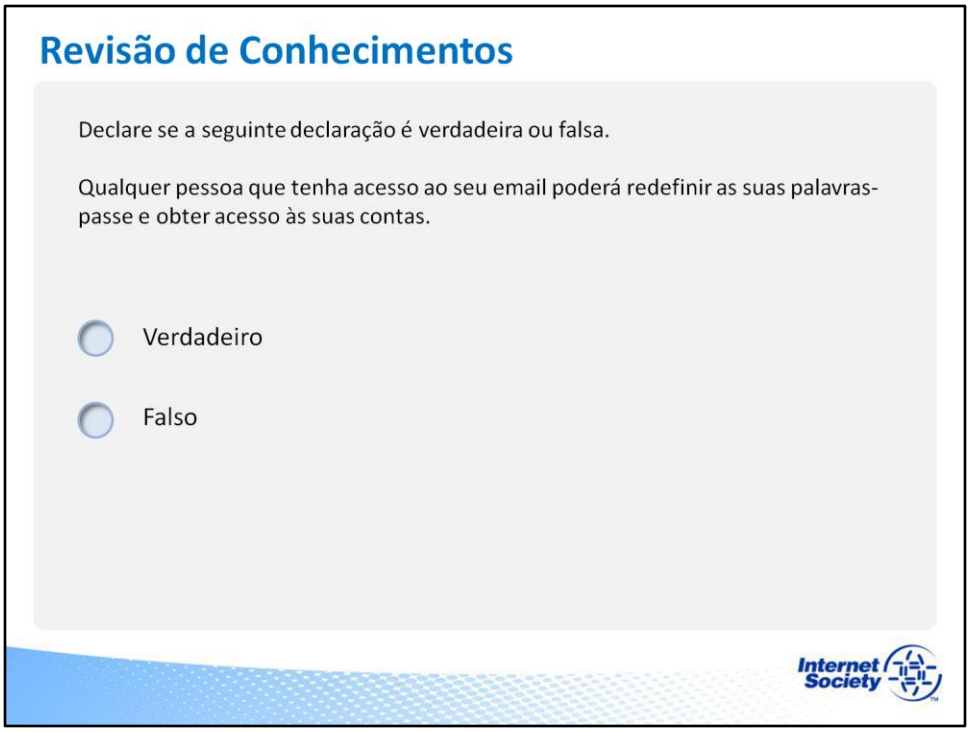
Selecione tudo que se aplica.
Em quais das seguintes situações a sua identidade *online* corre o risco de ser furtada?



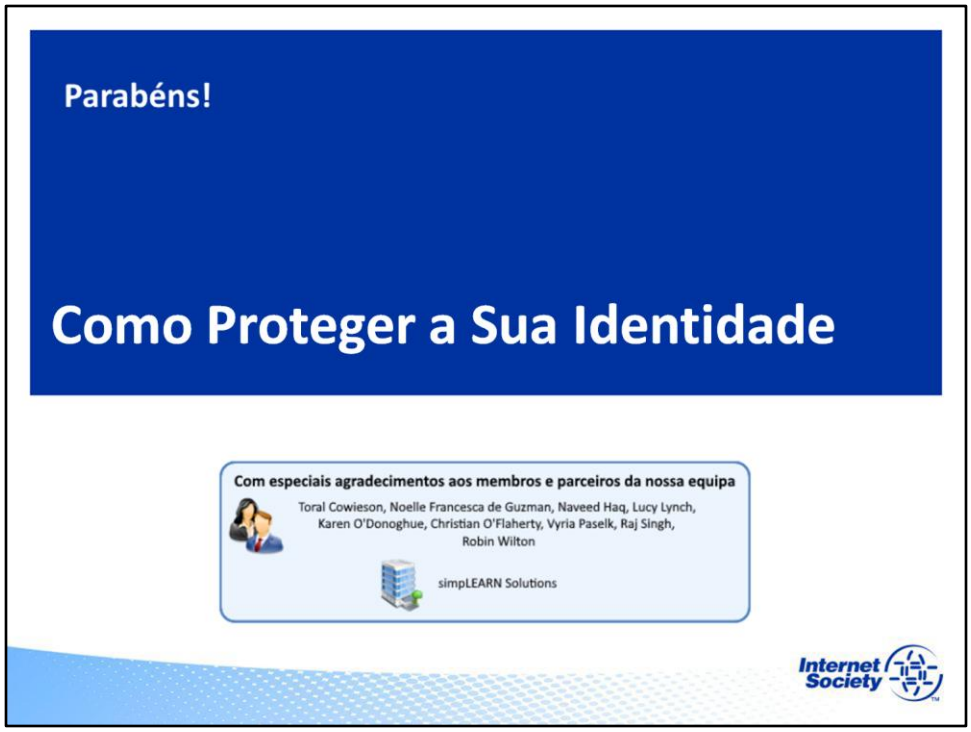
Indique se a seguinte declaração é verdadeira ou falsa.
A sua identidade *online* não é apenas valiosa para si, mas também para os seus fornecedores de serviços, como o seu banco ou um site de redes sociais.



Qual das seguintes opções se deve lembrar ao selecionar palavras-passe?



Indique se a seguinte declaração é verdadeira ou falsa.
Qualquer pessoa que tenha acesso ao seu email poderá redefinir as suas palavras-passe e obter acesso às suas contas.



Parabéns! Completou Gestão da Identidade, módulo 3 - Como Proteger a Sua Identidade.
Pode clicar em qualquer um dos separadores à sua esquerda para rever qualquer uma das partes deste módulo.