Welcome to the Protecting Your Identity Training Module
Introduction

Does loss of control over your online identities bother you?
Objective

By the end of this module, you will be able to:

• Identify the challenges in protecting online identities
• Recognize the ways in which you can protect your identity
Value of Your Partial Identity

Your identity has value, as does each of your online partial identities. Your identity is valuable not only to you but to others as well.

<table>
<thead>
<tr>
<th>YOU</th>
<th>SERVICE PROVIDER</th>
<th>ILLEGITIMATE USERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>The identity reflects you and gives you access to the resources you desire.</td>
<td>They are the holders of the resources you want. Your identity value is a business asset to those entities.</td>
<td>They want to access resources they are not entitled to.</td>
</tr>
</tbody>
</table>
What is Identity Theft?

Identity theft, broadly, is the loss of control over one or more of your partial identities.

As any online partial identities may contain private data, it is important to manage and protect them appropriately.

Most identity theft is an ‘enabling step’ towards identity fraud; reflecting the direct monetary value of some partial identities.
How does Identity Theft Occur?

Identity theft can happen in several ways. The types described here are common and happen to someone, somewhere, every day:

1. You are deceived into disclosing important personal information to the wrong person.
2. Someone (or some entity) is able to guess one or more of your passwords, or reset a password by exploiting password-recovery procedures, thereby unlocking your online identity.
3. Someone (or some entity) is able to eavesdrop on you electronically or take control of your computer without your knowing.
4. Mass data breach: usually a bulk compromise of a whole database of passwords at a poorly-secured third party site.
5. Parallel lives: an attacker gathers enough personal data to set up a new partial identity in your name - usually so as to get credit and then default on the loan.
Disclosing Sensitive Information to the Wrong Person

This form of theft is also called a ‘social engineering’ attack.

If a malicious website can persuade you that it is your bank or a trusted online merchant, you may be tricked into revealing sensitive data you would not otherwise have disclosed.

Social engineering attacks play on the user’s trust to trick them into inappropriate actions.
Spams and Phishing

A significant portion of the unsolicited email or “spam” sent to Internet users is designed to steal personal information.

These “phishing” messages try to convince you to connect to a malicious website designed to steal your identity, or disclose other data such as payment details, in the mistaken belief that you’re dealing with a trustworthy site.
Guessing /Resetting Your Password

This is a more sophisticated form of theft. It usually requires the ability to combine social engineering with weaknesses in online systems.

Most people choose passwords that can too easily be guessed. Sometimes, guessing at a password isn’t even necessary if the system has an automated password-reset feature.

If your password can easily be guessed, or it can easily be reset, you are at risk of identity theft.

You should also insist on secure browser sessions by default, so that your password is protected in transit.
Eavesdropping on you Electronically

This is a more technologically sophisticated form of theft.

It usually depends on malware (such as a virus) taking control of a computer or a computer network and then hunting for sensitive information, such as credit card numbers, online usernames and passwords, and so on.
Mass data compromise occurs when hackers are able to get hold of the password database from a service-provider’s website, and/or retrieve other data such as payment details, shipping address etc..

Such data, especially credit card details, is often then re-sold online through an organized, international black market.
Parallel Lives

This form of identity theft happens when an attacker gathers enough data about you to set up a bogus partial identity in your name. Usually this is a precursor to identity fraud.

This is a hard concept for some defrauded lenders to deal with.

Often when a victim of “parallel lives” tries to report the fraud, the system is weighted against the person whose identity has been stolen.
Inadequate Security Measures

When passwords are stored at service-provider websites, you have to rely on the security measures of the service provider. Poorly-managed databases can be attacked. Unfortunately, this is beyond the control of the user.
Protect your Online Identity

A little education and some common sense are the most important tools you have to avoid divulging sensitive personal information to individuals or entities that plan to exploit it.

- There are some technologies that can help.
- Consider adding plug-ins to your browser.
- Act on the warnings the plug-ins gives you.
Protect your Password

• Select passwords that you can easily remember, but that aren’t easy for other people to guess.
• Avoid using the same password for multiple websites. So, if one website is compromised, your stolen credentials can’t be used at other sites.
• Try customizing the password for each site by adding a few characters.
• Choose different, hard-to-guess passwords for each of the websites that are especially important to you, such as online financial services.
• If your bank offers two-factor authentication, you should consider using that.
Don’t Let Others Reset your Password

Password resets are meant to help you when you’ve lost a password (or have been locked out).

**Common Steps for Resetting Passwords**

1. You ask for your password to be reset, often by answering some personal “security” questions you have previously answered.

2. You may receive an email with a link that enables the reset or a new password might simply be emailed to you.

**Tip**

For websites that use security questions to validate your identity, use factual information (which makes it easy to remember) in ways that are difficult to guess.

Choose questions that have a unique meaning for you. For example, “Where did I lose my snowshoes?”
Protect Access to your Email

With password resets, it is important that you protect your email because your email address is often critical to the reset process.

Anyone who has access to your email may be able to reset your passwords and gain access to your accounts.

Protecting access to your email is one of the most important tools for protecting your online identity.

In particular, if your primary email account offers two-factor authentication, it is worth considering the extra layer of protection for this sensitive asset.
Common Techniques for Protecting Emails

The three common techniques adopted by most Internet users for protecting themselves online are:

• Logging out of accounts when they’re done.
• Using encrypted protocols (such as https or SSL protected email)
• Changing passwords periodically.

Some email services also offer you the option of multiple passwords.
Best Practices to Protect Email

Here are some good practices you can adopt to help protect your email, which helps protect your online identity.

1. Select email addresses wisely
2. Use reliable, secure email-forwarding services
3. Select different email addresses for each of your multiple online personae
4. Use 2-factor authentication wherever available
Use Email Addresses Wisely

As far as possible, choose email providers that have a good reputation for security and are established businesses likely to stay around.

Example

Using a free account provided by a local Internet Service Provider (ISP) might be a poor choice—unless you plan to never move or change ISPs ever again.

Consider segregating your email addresses

You may want to use one account for personal email traffic, while keeping a separate address for those times when a website asks you for one. That address need not personally identify you, but could be something like cannyshopper@mailservice.com. Some email providers will let you define multiple email addresses, so you can segregate further - perhaps one for shopping and one for your interactions with public sector services.
Use Reliable, Secure Email-forwarding Services

Use email-forwarding services, such as ones provided by professional associations or alumni associations, or commercial forwarding providers.

**Why use email-forwarding services?**

Email-forwarding services ensure:

- Your email address can remain consistent, even if you change where your email is delivered.
- There is an additional level of security against someone guessing or resetting your password, because your true email account is hidden.

However, you must also weigh this against the risk that the forwarding service might become unavailable over time.
Select Different Email Addresses for each of your Multiple Online Personae

When you have multiple online personae, such as professional, personal, and academic, select a different email address for each.

Why use different email addresses?

Carefully choosing the right persona when someone asks for your email address can prevent problems later on.

For example, your work or school email may not be very private if the company or institution claims the right to read or archive email on their servers.
Use 2-factor Authentication

Passwords alone cannot guarantee protection to your online identity.

2-factor authentication is a multi-layered security process. It combines different authentication techniques to make it more difficult for an attacker to compromise the whole authentication process. For instance, it may combine "something you know" (like a password) and "something you have" (such as a phone - which also means the authentication process can make use of two separate communication methods). This kind of 2-factor authentication would work as follows:

How it Works
1. Enter your password.
2. A second code is then sent to your phone.
3. Only after you enter this code you get access to your account.
Useful Resources

Useful Technologies

Latest versions of most Web browsers have the ability to check websites and alert you to ones that are known to be malicious.

Useful Links


The Online Trust Alliance website at https://otalliance.org/ has a resource list to help you learn more about the technologies that can help protect your identity on the Internet.
The Way Ahead

The technical and business communities supporting the Internet are working hard to remedy the patchwork of identity systems we have today.

**Creation of Trusted Identity Providers**

In a well-designed identity model, a user maintains one username and password (or another type of access credential, such as a hardware password token) with a single provider and that password is only given to that provider—never to any third party.

**Developing Internet Protocols**

There is work to develop Internet and browser-level protocols which will allow you to safely conduct distributed transactions without having to share your password or private information with all the websites involved. Existing protocols for federated identity make this possible. There are also newer initiatives on the secure exchange of individual attributes for authorization decisions, and the establishment of user-controlled ‘data brokers’.
Knowledge Check

Select all that apply.

In which of the following situations will your online identity be at risk of being stolen?

- You divulge personal information to a website that looks exactly like the website of your bank.
- You use a single password that is easy to remember for all your online identities.
- You find an interesting mail in your inbox, you open it and visit the website that asks you to download an executable file.
- You use multiple email IDs for your multiple online personae.
Knowledge Check

State if the following statement is true or false.

Your online identity is not only valuable to you but also to your service providers, such as your bank or a social networking site.

- True
- False
Knowledge Check

Which of the following you should remember while selecting passwords?

- Select passwords that you can easily remember.
- Select passwords that are hard to guess.
- Customize passwords for each site by adding a few characters.
- Use the same password for multiple websites.
Knowledge Check

State if the following statement is true or false.

Anyone who has access to your email may be able to reset your passwords and gain access to your accounts.

- True
- False
Conclusion

You have reached the end of the Protecting Your Identity training module.

You can click on any of the links on the left to review any section that you might like.

To learn more about this topic, click here.

Note to Reviewer: Please provide the link/url where the learner will be directed to learn more about this topic.