Understanding your Online Identity:
Learning to Protect your Online Identity

Your identity has value, as do each of your online partial identities. When the partial identity is with your bank or brokerage house, it may have clear monetary value. Other times, such as with social networking sites like Facebook or MySpace, the value may be less tangible, but just as important to you. Simply by being an active Internet user, you may find that you accumulate tens or even hundreds of these online partial identifies. *Identity theft,* the loss of control of one of your partial identities, is a natural concern, especially as the value of these identities grows, making them more attractive to thieves.

At the same time, because each of your online partial identities contains some information that may be very private, protecting yourself from a *loss of privacy* is often equally important.

This paper explores challenges in protecting online identities, gives ideas you can use to protect your identity, and discusses ongoing work in the Internet community to give you more control over your identity.

How can identity theft occur?

Identity theft can happen in several ways. All are common, and happen every day:

- you may be deceived into giving your identity information to the wrong person, or
- someone may be able to unlock your online identity by guessing your password or resetting your password by exploiting password recovery procedures, or
- someone may be able to eavesdrop on you electronically or take control of your computer

The first type of identity theft, giving your identity to the wrong person, is easy to understand because it ends up being simple theft. If you connect to a web site and give it your personal information thinking that it is your bank or an online merchant—but it isn't—then your information was simply stolen. A significant portion of the unsolicited email ("spam") sent to Internet users is designed to steal personal information. These "phishing" messages try to convince you to connect to a malicious web site designed to steal your identity.

The second common type of identity theft, having your password guessed or reset, is more sophisticated, because it combines social engineering with weaknesses in particular online systems. Unfortunately, most people choose passwords that can be easily guessed with a little thought and some patience. Sometimes, guessing the password isn't needed when there is a password reset procedure. For example, many online systems let anyone reset your password if they know a few facts about you, something Sarah Palin found out while running for US Vice President. If your password can be guessed easily, or be easily reset, you are at risk of identity theft.

The third common type of identity theft is more technical, because it usually depends on malware (such as a virus) taking control of a computer or a computer network and hunting for sensitive information such as credit card numbers, online usernames and passwords, and so on.

How can I learn to avoid giving the wrong person my identity?

Education and common sense are the most important tools you have to avoid giving your identity information to a malicious person. The US Federal Trade Commission is a good place to start, even if you don't live in the US. You can go to its web site at http://www.ftc.gov/idtheft for an extensive education program in English and Spanish to educate consumers about avoiding identity theft.

There are also some technology initiatives to help in this area. For example, recent versions of most web browsers include the ability to check web sites against a reputation database to help alert you to ones that are known to be malicious. The Online Trust Alliance (https://otalliance.org/) has a resource list to help you learn more about technology to help increase your confidence in using your identity on the Internet.

How can I keep someone from stealing my password?

If your password is easy to guess, then it is easy to steal. The most important thing you can do is select passwords that you can easily remember, but aren't easy for other people to guess. You should also avoid using the same password for multiple web sites, so if one site is compromised, your stolen credentials can't be used for other sites. Remember that you don't have to lose the password--the site you are using could have been compromised and your password for that site revealed. If you want to select passwords that are related to make them easy to remember, try to customize the password for each site by adding a few characters (such as the site name). This won't fool a dedicated attacker, but it will keep out someone who automatically tries your password on other web sites. You don't have to be too imaginative for many sites, but be especially careful to choose different, hard-to-guess, passwords for each web site that is especially important to you, such as online financial services. Many web sites--especially those holding financial or health information--employ various techniques to thwart thieves from trying to force their way into your account. One defense automatically locks an account when there have been too many login failures, which might indicate that someone is trying to guess your password.

How can I keep someone from resetting my password?

Password reset is used to help you keep control of an online account when you've lost the password (or have been locked out). Every web site has a slightly different technique, but the general idea is that you ask for your password to be reset, often by answering some personal "security" questions you've previously answered. Then you may receive an email to complete the reset process, or the new password might simply be emailed to you.

If the web site uses security questions, one good idea is to lie. For example, if the question is about the first school you attended or your first address, answer with the second school or address. That way, even someone who has access to a lot of information about you won't be able to answer the questions.

You also must protect access your email. Because your email address is often critical to the reset process, anyone who can read your email may be able to reset many of your passwords and gain access to your accounts. **Protecting access to your email is the most important tool to protecting your online identity.**

If access to my email is important, how can I protect my email?

Most Internet users know basic techniques to protect themselves online, such as remembering to log out of accounts when they're done, using encrypted protocols (*e.g.,* https or SSL-protected email), and changing passwords periodically. Here are some less well-known best practices you could adopt to help protect access to your email, which helps protect your online identity.

Advice	Why?
Use long-lived email addresses; select trusted email providers who will be in business a very long time. For example, using a free account provided by your local ISP is a poor choice—unless you plan to never move or change ISPs ever again.	The Internet isn't going away anytime soon, and you will want to create email accounts you hope you can use for decades to come. A single master email address will make it easy for you to reset forgotten passwords, and reduce the chance someone will be able to steal your identity by logging into a long-forgotten account.
Use reliable, secure email forwarding services, such as ones provided by professional associations or alumni associations, or commercial forwarding providers.	Email forwarding services ensure that your email address never changes, even if you change where your email is delivered. They also provide an additional level of security against someone guessing or resetting your password, because your true email account is hidden.
When you have multiple online personae, such as professional, personal, and academic, select a different email address for each.	Carefully choosing the right persona when someone asks for your email address can avoid problems later on. For example, your work or school email may not be very private if they claim the right to read or archive email on their servers.

Isn't there a better way to protect my identity online?

Yes… and no. The technical and business communities supporting the Internet are working hard to remedy the patchwork of identity systems we have today. They understand that we are operating on a system that wasn't specifically designed to manage identity, with significant breaches likely to continue—costing Internet users and companies time and money. But these solutions are being developed and aren't ready yet.

The model we are moving towards involves the creation of trusted *identity providers*, organizations that are part of the Internet infrastructure, just as email service providers and internet access providers are today. In a well-designed identity model, you maintain a username and password (or another type of access credential, such as a hardware password token) with a single provider, and you only ever give your password to the provider—never to any third party. If you've used an online merchant who supports payments with PayPal, you've seen this idea in action for payments. The same concepts can be used to protect your identity.

At the same time, open protocols in development in the Internet community will allow you to safely link your identity at different web sites together without having to share your password or private information between the web sites. These technologies will be invisible to you, but they will improve security by working to keep your identity safe. You'll have the rich, customized Internet experience you want, but not at the cost of losing control of your privacy and identity.

About the Internet Society

The Internet Society (ISOC) is a nonprofit organization founded in 1992 to provide leadership in Internet related standards, education, and policy. We are dedicated to ensuring the open development, evolution and use of the Internet for the benefit of people throughout the world.

Internet Society™