Understanding your Online Identity

Learning to Protect your Identity

Your identity has value, as do each of your online partial identities. When your partial identity is with your bank or a brokerage house, for example, it may have clear monetary value. When it is with a social networking site, such as Facebook or MySpace, the value may be less tangible but equally important to you. Simply by being an active Internet user, you may find that you accumulate tens or even hundreds of online partial identifies.

Identity theft, which results in a loss of control over one or more of your partial identities, is a natural concern; as the value of your partial identities grows, the information becomes more attractive to thieves. At the same time, because each of your online partial identities contains some information that may be very private, generally protecting yourself from a loss of privacy is often equally important.

This paper explores challenges in protecting online identities. It offers ideas you can use to protect your identity and it discusses ongoing work in the Internet community that may help give you more control over your identity.

How can identity theft occur?

Identity theft can happen in several ways. The three types described here are common and happen every day:

- You are deceived into disclosing important personal information to the wrong person
- 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
- Someone (or some entity) is able to eavesdrop on you electronically or take control of your computer without your knowing

The first type, giving sensitive personal information to the wrong person, is a relatively simple form of theft. If you connect to a website and divulge personal information because you believe it to be your bank or a particular 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 website designed to steal your identity.

The second type, having your password guessed or reset, is more sophisticated because it requires the ability to combine social engineering with weaknesses in online systems. Unfortunately, most people choose passwords that, with a little thought and some patience, can too easily be guessed. Sometimes, guessing at a password isn't even necessary if the system has an automated password-reset feature. In fact, many online systems allow anyone to reset a password as long as a few facts about the account holder are known, something former U.S. Governor Sarah Palin found out when she was running for vice president. If your password can easily be guessed, or it can easily be reset, you are at risk of identity theft.

The third type is more technologically sophisticated because 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.

How can I learn to avoid giving the wrong person my 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. The U.S. Federal Trade Commission is a good place to start, even if you don't live in the United States. The website at http://www.ftc.gov/idtheft contains useful information in English and Spanish aimed at educating consumers about avoiding identity theft.

There are also some technologies that can help. For example, newer versions of most Web browsers have the ability to check websites and 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 the technologies that can help protect your identity on the Internet.

How can I keep someone from stealing my password?

If a 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 that aren't easy for other people to guess. You should also avoid using the same password for multiple websites, so if one website is compromised, your stolen credentials can't be used at other sites. If you want to select passwords that are related to make them easy to remember, try customizing 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 anyone who tries your password on other websites. Be especially careful to choose different, hard-to-guess passwords for each of the websites that are especially important to you, such as online financial services. Many websites—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 resets are meant to help you when you've lost a password (or have been locked out). Every website has a slightly different technique for resetting a password, but the general idea is that you ask for your password to be reset, often by answering some personal "security" questions you have previously answered. Then you may receive an email with a link that enables the reset or a new password might simply be emailed to you.

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. For example, if the question asks for the name of the first school you attended or the name of the first street you lived on, answer with the second school you attended or the second street you lived on. That way, even someone who knows a lot about you will have trouble answering the questions.

With password resets, it is important that you protect your email because your email address is often critical to the reset process; in other words, 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 the most important tool to protecting your online identity.

If access to my email makes me vulnerable, how can I protect my email?

Most Internet users know basic techniques for protecting themselves online, such as remembering to log out of accounts when they're done, using encrypted protocols (such as https or SSL-protected email), and changing passwords periodically. Table 1 has some less-well-known best practices you could adopt to help protect your email, which helps protect your online identity.

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 was not specifically designed to manage identity. Unfortunately, significant security breaches are likely to continue, costing Internet users and companies both time and money. Many solutions are still under development.

The model we are moving toward involves the creation of trusted identity providers. These are 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, 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. If you have ever done business with an online merchant that uses PayPal, you have seen this idea in action. The same concept can be used to protect your identity.

Advice	Why
Use long-lived email addresses; select trusted email providers that are likely to be in business a long time. For example, using a free account provided by a 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 so you want to create email accounts you can use for decades to come. A single master email address will make it easy for you to reset forgotten passwords and it will reduce the chances that 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 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.

Table 1: Best Practices to Protect Email

At the same time, open protocols that are under development in the Internet community will allow you to safely link together your identity at different websites without having to share your password or private information with each of the websites. These technologies will be invisible to you but they will improve security by working to keep your identity safe. You will 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™