ITS Communications

Algonquin College
Cybersecurity Awareness Month
2024

Protecting Your Identity

In today's world, would-be thieves have more ways than ever to steal your information. Attackers have used phishing emails for quite some time now, but with so much of your information potentially accessible online, it's harder than ever now to keep your identity secure.

What is it?

Identity theft is the fraudulent acquisition of your personal information - full name, date of birth, social security number, credit-card information, etc. - by another individual or criminal organization. This can be accomplished in a number of ways, which we will touch upon later.

Once an attacker has your information, they can use it to impersonate you; how effectively depends on just what they have obtained. Damages can range from attacks on your social-media profiles to complete destruction of your credit through fraudulent loans and purchases.

Where can they get my information?

The truth is anything at all with personal information can be used against you. Identity thieves still obtain information the old-fashioned way - through physical means. Most people are conscious of their purse or wallet, but some of the most damaging information can be found in unconventional places, like:

- An unlocked car
- Receipts tossed in the trash
- Conversations overheard in public
- Physical mail or packages
- An automated-teller machine (ATM)

With the rising popularity of the Internet, attackers now have a number of ways to obtain your information digitally, as well. Below are some of the common tactics used by online attackers today:

- **Spear phishing** – Spear phishing uses fraudulent emails and relies on the victim clicking a link in the message, opening an attachment, or putting information into a fraudulent website.
- **Pharming** – Pharming deceives the victim by hijacking a real website or domain name server (DNS) and redirecting him/her to a duplicitous one run by the attackers.
- **Pretexting** – Also known as blagging, this technique engages the victim through a variety of media, such as email, social media, and telephone.

In most cases, the best way to protect your identity is to be cautious of whom you share your information with. It's much easier to obtain your information through you than to obtain it illegally, so you are your own first line of defense. On your right are some tips for keeping your information secure.

It's difficult to keep your information 100% secure, but by remaining vigilant, you can prevent or mitigate most attacks before they do any damage. Remember that legitimate organizations will never ask for your password or other sensitive information via email; if you spot suspicious activity, make sure to report it using the Report Phishing Button or to spamorscam@algonquincollege.com.

Ways to better protect your identity
The following practices will keep you more secure:

- Keep your documentation in a secure place; shred old documents rather than discarding them.
- Encrypt computer files containing sensitive info.
- Activate multi-factor authentication on your accounts.
- Use unique passwords for each account and change them frequently.
- Avoid unsecured, public networks, or connect through a VPN.
- Check your bank statements and credit score regularly.

Information Security & Privacy is Everybody's Business