While the Internet has transformed and greatly improved our lives, this vast network and its associated technologies have opened the door to an increasing number of security threats from which we must protect ourselves. The consequences of attacks can range from the mildly inconvenient to the completely debilitating. Important data can be lost, privacy can be violated and your computer can even be used by an outside attacker to attack other computers on the network.

The following are some tips to keep in mind to help protect your identity and data.
Choosing a secure password is the first step towards protecting your data and identity online. According to traditional advice, a strong password –

- Contains at least 12 characters.
- Includes a mix of numbers, symbols, capital and lowercase letters.
- Isn’t a dictionary word or combination of dictionary words.
- Doesn’t Rely on Obvious Substitutions: Don’t use common substitutions, either — for example, “H0use” isn’t strong just because you’ve replaced an o with a 0.
Phishing

IT would like to take this opportunity to remind users to be vigilant of the email messages that land in their inbox – especially those messages that ask you to divulge personal information. These messages are examples of phishing attacks. Phishing attacks use spoofed emails and fake web sites to fool the recipients into divulging personal information such as user names and passwords, credit card numbers, social insurance numbers, etc.

The easiest way to protect yourself is to never respond to anyone who asks for personal information by email, even it is from a seemingly legitimate source.

Be suspicious of any email that:

- Asks you to divulge personal information.
- Isn't personalized (uses generic greetings such as 'Dear Customer').
- Has links that don't match what is displayed (when you hover over the link with your mouse).
- Has a false sense of urgency.
- Is poorly written.
What does a phishing email look like? Here’s some examples -

Hello,
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Our system detected unusual Copyrights activity linked to your Facebook account, please follow the link below to fill the Copyright Law form:

http://www.facebook.com/application_form

Note: If you don’t fill the application your account will be permanently blocked.

Regards,

Facebook Copyrights Department

From: kmanagement@amazoncanada.ca on behalf of sheridan@can.ca
To: @sheridan@can.ca
Subject: Suspension

Dear Client,

We have sent you this e-mail, because we have strong reason to believe, your account has been used by someone else in order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.

We’ve locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link below:


Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates

not an Amazon e-mail address
(note the missing A in Amazon)

Links in email

Spelling

Threats

Popular company

Generic non-personalized greeting

Hovering over the link reveals it points to a non-Amazon site - “http://redirect.kereskedj.com”
Malware, short for malicious software, is any software used to disrupt computer operations, gather sensitive information, or gain access to private computer systems.

How can I avoid Malware?

- Install anti-virus/malware software. Examples – Malwarebytes, Ad-Aware.
- Keep your anti-virus software, operating system, and browser up to date.
- Secure your Wi-Fi network. Make sure it requires a password to access it and that the password is strong. Use WPA or WPA2 encryption.
- Avoid using unsecure Wi-Fi networks such as those in restaurants, airports, etc.
- Always use a firewall. If you are not running a third party firewall, use Windows Firewall. Do not run two firewalls at once as they may interfere with each other.
**Firewalls**

What is a firewall?

A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

Why is a firewall important?

- The firewall system is designed to prevent unauthorized access to or from a private network. If you use a computer at home or work, the most effective and important first step you can take to help protect your computer is to turn on a firewall.

- Windows 8, Windows 7, Windows Vista, and Windows XP SP2 or higher have a firewall built-in and turned on by default.
How to check if your Windows Firewall is on -

1. Go to Start → Control Panel → Windows Firewall.

2. This is what the window should look like if your firewall is turned on –
Antivirus Software

Antivirus or anti-virus software sometimes known as anti-malware software, is computer software used to prevent, detect and remove malicious software. Antivirus software was originally developed to detect and remove computer viruses, hence the name. However, with the proliferation of other kinds of malware, antivirus software started to provide protection from other computer threats.

Antivirus do’s and don’ts -

- Do run the antivirus program in full-time, background, automatic, auto-protect, or similar mode.

- Do enable Macro Virus Protection in all your Microsoft Office programs.

- Don't allow your e-mail programs to "auto open" attachments.

- Don't open attachments from people you don't know or attachments that seem suspicious.
Spam

What is spam?

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender.

How does spam work?

At its simplest, spam is the mass mailing of a single email to thousands, millions or billions of recipients. The spammer obtains a list of valid email addresses from one of several sources and then fires out as many emails as they want, hoping to get one or two percent of profitable responses.
How do I avoid spam?

• Keep your email address to yourself as much as possible.

• When posting on a forum, do not include your email address as part of your signature.

• Review privacy terms on websites before registering.

• Do not use the unsubscribe links in spam emails, in some case that will actually confirm the email address is valid to the spammer.

• Never click on links in spam email.

• Do not open attachments in spam, you could get infected with Trojans that will send your email contacts to a spammer as well as entrap you in a spammer distribution chain i.e. your computer might be the one that the spammer uses to send spam emails.