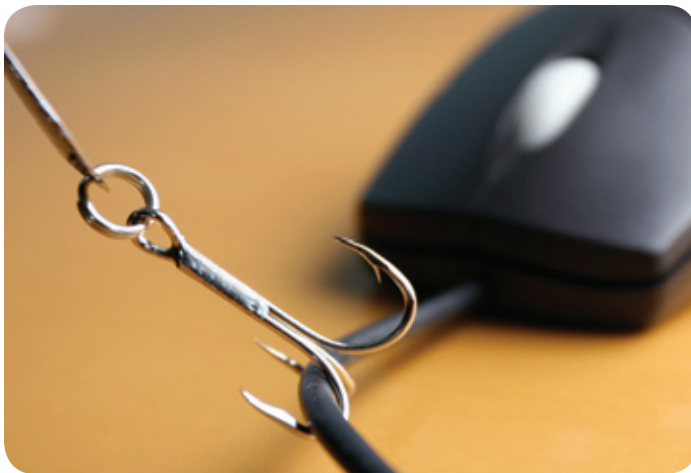


# PHISHING

HOW TO **RECOGNIZE IT** AND  
BETTER **PROTECT YOURSELF**



## What is Phishing?

Phishing is an online scam where fraudsters impersonate a trusted person or organization in an attempt to obtain personal information that may be used for identity theft.

## Forms of Phishing

Scammers send emails pretending to be from a legitimate retailer, bank, organization or government agency. The emails generally ask you to confirm your personal information by clicking on a link to a phoney website where you are asked for personal information such as identifiers or passwords. The websites may look very similar to a real company or organization you deal with on a regular basis. Sometimes you can tell that a website or email is a false one if there are spelling and grammatical errors. Websites or emails from legitimate companies should not contain spelling and grammatical errors.

## Signs of Phishing

Phishing can take many forms and recognizing the signs can help protect you from identity theft. A fraudulent email can often seem innocent or even helpful. For example, the email sender could be contacting you for the following reasons:

- your account or credit card is about to be closed
- an order for something has been placed in your name
- your personal information has been lost because of a computer error or breakdown
- there is suspicion that your account or credit card has been subject to fraud

The giveaway is that the email will ask you to supply personal information that could be used to create a false identity or to impersonate you (such as asking for your account numbers, passwords or other sensitive personal information).

## Protect Yourself

### **Never respond to an email asking for your personal information.**

Phishers often send authentic looking messages that appear to come from legitimate companies requesting personal information or asking you to confirm personal information which is then used for fraudulent purposes. Do not respond to email claiming to be from, for example, your financial institution or other legitimate organizations, asking you to provide your passwords, financial information or other personal information. Your bank should never send you an email asking you to provide this information. Even though your bank may call you if they suspect fraudulent activity on your bank account or credit card, they should never ask you to provide your passwords or account numbers verbally or via the telephone keypad.

If you are asked for this type of information, phone the organization to verify that the request is valid, but **do not** use the email address or telephone contact information provided in the email as it could be false as well. Instead, look up the contact information for the organization on their website, in the phone book or on printed correspondence you may have from them.

### **Never enter your personal information in a pop-up screen.**

Phishers can direct you to a real company's website, but then an unauthorized pop-up screen created by the phisher will appear asking you to provide personal information. Legitimate companies do not ask for personal information via pop-up screens.

### **Never open email attachments from someone you don't know.**

Even if the message looks like it came from someone you know, it could be from phishers, trying to steal your information. If you are not expecting an email attachment from someone, verify with that person before opening it.

### **Install anti-virus and firewall software.**

Phishing emails may contain software and computer viruses that can harm your computer or track your activities on the Internet without your knowledge. Many Internet Service Providers (ISPs) in Canada provide security software to their customers for free.

**Anti-virus software** can help protect your computer from computer viruses. It can also help remove known viruses from an infected computer system. Make sure you choose anti-virus software that is up-to-date so that it recognizes current and old viruses.

A **personal firewall** is a software package that helps you control information that is received and sent from your computer. Make sure to choose a firewall that provides protection for information you receive (incoming) and information you send (outgoing).

### **Update your anti-virus program and personal firewall regularly.**

New computer viruses are found every day. Many software packages allow you to check for viruses and download updates automatically (auto-update). You may be able to find more details on how to update your software in the information available with each software package.

## **How to Fight Phishing**

There are ways to fight phishing and they start with your Internet Service Provider (ISP). Most ISPs have filtering tools that scan emails before they reach your computer and automatically get rid of known phishing emails. Most ISPs offer this service, sometimes for a monthly fee.

It is important to also set up your own filtering service on your email account. Many free email services offer these filtering services. You can also download many phishing filters or anti-phishing programs for free by searching the Web. Ensure that you only download programs from trusted sources.

Some financial institutions and credit card companies offer online examples of what phishing emails look like. Some may also offer specific email addresses where you can send any phishing emails that you have received. Contact your financial institutions and credit card companies by telephone or visit their websites for more information on the resources and services they offer to report phishing.