

## What is “Phishing,” and Why Should I Know More About it?

Phishing scams are now a part of everyday on-line life, so it's important that you know how to spot one... and avoid becoming a victim.

### Overview of Phishing Scams...

Phishing scams are just another attempt to get valuable, personal information. Scammers send mass e-mails to every address they can find. Typically the message will appear to come from a name bank or financial institution, PayPal, Amazon, etc. The e-mail typically asks you update your information for one reason or another, and they usually provide a link you can 'click' on to do so.

This all sounds reasonable, and the-mail is usually very convincing... but they're anything but legitimate. The link provided **doesn't** take you to the name company's website, rather you'll be submitting your information to a website run by scammers with malicious intentions.

### Why Scammers Use Phishing Scams...

Why would anyone do this? Well, with a phishing scam it's easy to gather a lot of juicy information... like account numbers and passwords. From there it's not that hard to steal your bank balances.

Some phishing scams will ask for personal information (SIN numbers, mother's maiden name, date-of-birth, drivers license information, etc) so that they can steal identities and open credit accounts in the victim's name. Some victims of phishing scams have given up their credit card numbers only to find that the card was used fraudulently.

### Why People Fall for Phishing Scams...

Anybody can be tricked by a sophisticated phishing scam. Simple ones are easy to spot, but the best scammers are actually pretty smart. They use a variety of tricks to make the scam appear to be a legitimate process. For example, they might include a bank logo right on the email message or website. Or, the link provided in the e-mail may *look* like it goes to the bank's website, while in fact, the victim is actually sent to a very different site.

### How to Spot Phishing Scams...

It's easy to uncover a crude phishing scam. For example, if you get an e-mail from a bank you've never had an account with, then don't click on the link at all. If you actually have an account at the institution it can get more interesting.

You'll want to look at the message carefully to see if it could be a phishing scam. Are any words misspelled? Sometimes scammers operate from third-world countries, or English (or French) isn't their first language, so they may give themselves away by using poor spelling and grammar.

You should also examine the link they provide. Does it really go where it appears to go? For example, they could tell you that they're giving you access to the government's 'Top Secret Database' at <https://www.TopSecretDatabase.gov> but if you click the link you'll find that you've been directed to a different site.

You should never click on a link in a suspect message... rather copy the link and paste it into your Internet browser address line. But remember, you can still be tricked by web addresses that look legitimate, but have one or two letters switched.

The best way to avoid becoming a phishing scam victim is to use your best judgment. Recognize that no reputable financial institution will e-mail you asking you to provide personal or sensitive information. In fact, most institutions will tell you something along the lines of... "We'll *never* ask you for your personal information via phone or e-mail."

### If You Are, or Think You're a Victim of a Phishing Scam...

If you've been tricked by phishing scams in the past, you need to be vigilant. First, let your financial institution know what happened. They'll likely want to pursue the scammer, and they'll also monitor your account more closely. Next, let your credit card companies know about it by calling them. Finally, keep a close eye on your (postal service) mail and your account statements. If you stop receiving expected statements, or if you see unusual activity on them, call your bank immediately.

### How You Can Help Prevent Phishing Scams...

Let's all work together to prevent phishing scams. If you receive a suspicious email, report it. You can send it to the <http://www.antiphishing.org>, or you can just click the 'Report as Junk' (or similar) button on your e-mail program.

**Courtesy of Ottawa Computer Services**  
[www.OttawaComputerServices.com](http://www.OttawaComputerServices.com)

**613.296.7777**