Phishy e-mail? Don't take the bait

A few months ago Canada Revenue Agency issued a notice about a scam in the United States where taxpayers were receiving an unsolicited e-mail that appeared to be from the Internal Revenue Service saying they had been selected for an "electronic audit."

The intended victims were told to click on a link to an IRS Web site where they were instructed to download a form and fill in their bank account numbers and other financial and personal information.

They had to return the form within 48 hours to avoid penalties and interest.

It all appeared very authentic and official.

Except the site wasn't run by the IRS and there is no such thing as an "e-audit."

Instead of communicating with the IRS, unwitting e-mail recipients were tricked into installing malicious software onto their computer and sending information that should be kept private to some very bad people.

This is an identity-theft scheme known as "phishing" (so-called because victims are lured by the promise of money or some other payoff). Some scams ask for your personal information directly while others refer you to a trustworthy-looking site where you're asked to verify your identity by entering personal information like your social insurance number.

Examples of e-mail scams circulating here recently include notifications that you're entitled to a tax refund and need to provide bank account numbers so the CRA can send you the money (the amount is always very specific, like $521.51 or $671.08). CRA never transfers money via e-mail; it will only send payments by direct deposit or by cheque.

Security tips

These CRA warnings about phishing are a great reminder to keep your personal information secure, especially with more and more tax correspondence – and financial transactions – taking place online.

Here are a few points to ponder:

• The CRA never uses e-mail, text messages, or voice mail to ask for personal information of any kind, including passport, health card, or driver's licence numbers. Nor will it divulge information about you to another person unless you provide formal authorization.

• If you receive an e-mail claiming to be from CRA asking for personal information, don't reply.

Don't click on any links, and do not open any attachments.

Forward the e-mail as-is to info@antifraudcentre.ca and then delete the original message.

• Phishing scams want you to act immediately. Watch out for e-mails with phrases like "urgent action required" or "you only have 72 hours to reply."

• Be wary of e-mails with a generic greeting like "Dear Taxpayer." Phishing is a high-volume scam.

Even though they may have your e-mail address, scammers seldom have your name.

• Make sure the Web sites you're using are secure.

Look for the prefix "https" and a locked padlock or unbroken key symbol.

Check the site's authenticity by double-clicking on the symbol. If in doubt, close your browser, reopen it, and type the web address for the site you want directly into the address bar rather than searching for it. This helps avoid being misdirected to a bogus site.

• Change your passwords regularly. Some CRA electronic services, such as NETFILE, require that you call CRA in order to change or replace a lost, misplaced, or compromised password.

Other services like My Account or My Business Account allow you change your login information online.

The CRA posts examples of fraudulent letters, e-mails, and online refund forms on its Web site: www.cra-arc.gc.ca/ntcs/bwr-eng.html.

You might think that few people would be fooled by spammy-sounding e-mails that are riddled with spelling mistakes and bad grammar, but a few is all a scammer really needs.

Perfect foil

The CRA is the perfect foil for a phishing scam because innocent people will give up their deepest, darkest secrets to avoid the threat of trouble with tax authorities.

If you get a suspicious e-mail, letter, or call and want to make sure it's from CRA, call the agency yourself at 800-959-8281 for personal services or 800-959-5525 for business services. Agents will be able to confirm whether any CRA department is looking to contact you.

When in doubt, ask yourself whether the request is for information that you wouldn't otherwise include with your tax return, or that you know CRA already has on file.

If the caller or e-mail needs to "verify" your social insurance, credit card, bank account, or passport numbers, don't take the bait. They're not with CRA.

Scott Taylor is vice-president of TFS Group, providing accounting, bookkeeping, tax return preparation, and other business services for owner/operators. Learn more at www.tfsgroup.com or call 800-461-5970.