Phoney phishing and pharming

Barrie McCombs, MD, CCFP, CCFP(EM)

Director, University of Calgary Medical Information Service, Calgary, Alta.

Correspondence to: Dr. Barrie McCombs, Director, University of Calgary Medical Information Service, 3330 Hospital Dr. NW, Calgary AB T2N 4N1; bmccombs@ucalgary.ca; www.ruralnet.ab.ca/medinfo/

Unfortunately, these terms do not refer to an idyllic rural lifestyle. They are Internet-based scams where a thief tries to steal your identity or raid your bank or credit card account.

For example, I recently received several email messages from the Royal Bank of Canada warning of security problems with my account. They said that I could correct the problem by logging into my account using an Internet address link in the message. They also include a number of handy tips about how I can avoid future security problems. There's just one problem — I've never had a Royal Bank account!

This is an example of "phishing," where a scam artist sends an email message to thousands of email addresses. They hope to find a few individuals who actually use the financial institution mentioned in the message and are naive enough to reply to the message with their bank account or credit card numbers, passwords or other personal information. If they do, the thief then tries to steal their identity, or withdraw money from their bank account.

Phish finding

The message looks very official, and often includes graphics that the thief has copied directly from the real institution's Web site. It is usually vaguely addressed to "Dear <your email address>" or "Dear Valued Customer," and will appear to come from a legitimate email address (e.g., support@rbc.com). There will be a sense of urgency to the message, implying some loss of service if you do not respond immediately.

Phoney Internet address

The message contains an official-looking, but false Internet address (e.g., https://login.royalbank.com). When I viewed the "source code" of the messages I received, the actual address was completely different than the one displayed. It was located, not in Canada, but in the Czech Republic. Most Canadian banks and credit card companies have encountered this type of scam. Articles about phishing stress that these institutions never send out this sort of email message.

Never click

Never click on the link or anywhere else inside the message. Even if you do not provide any personal information on the target page, the connection may enable the thief to download a "Trojan Horse" virus to your computer. This may allow them to steal personal information at a later time. You can minimize this risk by always keeping your anti-viral software up to date. This trick is known as "pharming."

Never reply

Never reply to the email message itself. That just confirms that your email address is still active and makes you the target for future scams.

Delete the message

Delete the message immediately. That prevents some other curious member of your family from making the mistake that you have hopefully avoided.

Report the scam

If you have a relationship with the bank or credit card company listed in the message, contact them to report the

scam. To be safe, look up their correct phone number in the phone book or on a previous financial statement. Or go to their real Web site, by typing in the address yourself.

Be sceptical

On a related note, never purchase anything offered for sale in an unsolicited email promotion, even if it appears legitimate. If you believe that the offer is real, write down the company's address and type it yourself. This avoids being redirected to a phoney Web site.

Password protection

Change your passwords frequently and include characters and numbers. For important Web sites involving financial information, do not use any software program (including MS Windows) that saves passwords. Always select the "log off" option at the end of a visit to a financial Web site. For extra security, clear your browser's cache memory immediately after the visit. You can do this in Internet Explorer by clicking on Tools > Internet Options > Delete Files. There is a similar feature in other browser programs. Another benefit of occasionally clearing this "cache file" is that it may speed up your browser's response time.

Canadian Bankers Association

The bilingual CBA Web site (www.cba.ca) contains excellent information about various ways to avoid identity theft. Click on the "protecting your personal information online" link. They also have a convenient list of their member institutions to help you report an attempted identity theft. Most financial institutions have additional security and contact information on their own Web sites.

Competing interests: None declared.