Continuing the series on cyber security that began in the April 2007 issue of *The ATA Chronicle*, this article will focus on the risks posed by phishing. Although the precise origins of the term are unclear, *phishing* is a play on the verb *fishing*. In fishing, one uses some form of bait in the hope of tempting fish to bite. If and when a fish finds the bait alluring enough to swallow, it is hooked and reeled in. Phishing operates on the same principles. However, the “bait” consists of deceptive e-mail messages designed to trick users into supplying confidential information such as online banking credentials, account numbers, or other sensitive information.

Ignorance of the threats posed by phishing has a steep price indeed, as those who fall for the bait and reveal sensitive personal data to phishers are at high risk of credit card fraud, damaged credit history, and identity theft. Repairing damage to credit history and/or recovering from identity theft can take months or even years. This article will thus explain some of the techniques used in phishing e-mails, and will provide some practical strategies to help translators recognize these deceptive messages for what they are and avoid being “reeled in” by phishers.

**Phishing and Its Lures: Spoofed E-Mail**

Phishing is based on the principles of social engineering, whereby infor-
Information hunters “deceive a trusted user into revealing information, or trick an unsuspecting mark into providing [them] with access to a machine, network, or account.” The motivation to phish is primarily financial, as phishers can either sell the stolen information or use it to commit fraud. It is thus not surprising that the financial services sector accounted for 84% of the brands that were phished during the second half of 2006. The phisher begins by crafting an e-mail “lure” that masquerades as a legitimate communication from a well-known financial services organization, such as a bank. The message may give every appearance of being an authentic e-mail from the bank, and may include items such as the bank’s official logo, trademarks, copyright notices, links to pages on the bank’s actual website, and more. The phisher may send out thousands or even millions of copies of the message in the hope that a few will find their way into the e-mail inboxes of legitimate account holders and trick them into believing that the message has in fact been sent by the bank. Alternatively, the phisher may conduct preliminary research to determine with which bank(s) a given victim does business, and then send the victim fake e-mail that appears to be from those institution(s). This targeted variant of phishing is sometimes referred to as “spear phishing.”

Whether the phisher takes a scatter-shot or targeted approach, the phishing e-mail message will typically advise users that there is a problem with their account and that they must reset their password or verify the security of their account information immediately in order to avoid problems, which may include a frozen account or blocked access. In the typical scenario, the e-mail will invite users to click on a hyperlink to “verify” their information. Clicking on the link causes a special dedicated page to load on which users are asked to “confirm” sensitive confidential information that may include some or all of the following: first and last names; address; date of birth; social security number; account number; user ID; password; PIN; mother’s maiden name (a security challenge question commonly used by banks to identify customers); and security code (the three-digit number stamped in the signature panel of credit cards used by merchants to confirm that the person conducting an online or phone transaction actually possesses the card). In this scenario, the webpage via which unsuspecting users “update” their confidential information is in fact a cleverly disguised trap designed to steal their information.

The Better the “Lure,” the Higher the Risk of Being “Hooked”

In some cases, an examination of the URL (address of the website) to which the e-mail hypertext link points will reveal the attempted trickery. For example, let us assume for the purposes of our discussion that we have received an e-mail that appears to be from “Trustworthy Bank.” If the message asks us to “verify our information” and supplies a link that does not point to the TrustworthyBank.com website, but rather to a different domain, such as bankphishers.com, then we can be pretty sure that the e-mail is illegitimate. The screenshot shown in Figure 1 shows a phishing e-mail received by the author on March 18, 2007.

Although the above e-mail appears at first glance to have been sent by Western Union, a close look at the hypertext link in the message reveals that the link does not point to the westernunion.com website, but rather to the amareviewteam.us website (which is not affiliated with Western Union, according to whois.nic.us domain registry data as of March 19, 2007).

Not all phishing attempts are as obvious as the above example. Instead of displaying the URL in the body of the e-mail message, where users might scrutinize it and notice that it points to a third-party site, many phishers take the deception a step further by “hiding” the fake URL behind hypertext link text that appears to be legitimate. For example, let us imagine that we have received an e-mail claiming to be from “Trustworthy Bank” that includes a hypertext link. Let us further imagine that the link text does not display a URL, but rather an invitation to the user to “click here to update your
information on the Trustworthy Bank.com website.” In this case, if we wish to find out what webpage the link points to, we can hover our mouse over the link and note the URL that displays in the status bar (in the lower left-hand corner of the browser) to see if it appears to be legitimate. The screenshot in Figure 2 shows a phishing e-mail received by the author on March 14, 2007.

At first glance, the link in the above message appears to point to the following URL:

https://www1.rbcroyalbank.ca/RBCUPDATE:XSDFV3GHI

In fact, if we hover our mouse over this link and examine the address that displays in the status bar, we will see that the link in fact points to a different URL altogether, as shown in Figure 3 on page 25.

Since the marijuanaforthemasses.com website is presumably not affiliated with the Royal Bank of Canada, the user is well advised to delete this message.

The Royal Bank of Canada phish below is a bit more sophisticated than the Western Union phish shown in the first example, since it integrates the actual Royal Bank of Canada Global Private Banking logo. Some phishers craft highly realistic messages that include authentic graphics and links to legitimate sites. For example, consider the phishing e-mail received by the author on 14 March 2007 shown in the screenshot in Figure 4 on page 25.

The message contains three hypertext links. The link in the lower left-hand corner of the message (“Equal Housing Lender”) points to a legitimate page on the bank’s actual website (see Figure 5, page 26).

However, the “Sign In” and “Sign In to Online Banking” links point to a third-party site that is presumably not affiliated with the bank (see Figure 6 on page 26).

A close look at the URL to which the sign-in links point reveals that although it does contain a reference to “bankofamerica.com,” it does not direct the user to a page on the Bank of America website, but rather to a page on the spiderjapan.com website. In order to determine the name of the website to which a link points, one simply needs to read from “http://” or “https://” until one reaches the first top-level domain (TLD) designator (.com, .net, .org, .biz, .edu, etc.; TLDs may also be country-specific, for
example, .de, .fr, and .jp). Because the URL in the sign-in link in Figure 6 on page 26 points to a page on the spiderjapan.com website, users would be ill advised to accept the message’s invitation to “click on [the link] to continue to the verification process and ensure [their] account security.” Although alert users might suspect that the e-mail is fake due to the relatively poor quality of the linguistic content, the quality of the graphic design—which includes official corporate and Olympic team sponsor logos—underscores the increasing sophistication and realism of phishing attempts.

In any event, examining URLs is not a foolproof strategy for identifying phishing messages. Some phishers create websites whose domain names are nearly identical to those of legitimate institutions, but which include subtle typos that may easily escape the user’s notice. The phishing e-mail shown in Figure 7 on page 27, which was sent to the author on March 19, 2007, contains a particularly insidious example of this type of deception: the reader will need sharp eyesight indeed to note that what appears to be a “w” in the first letter of “westernunion” in the link is in fact a pair of lower-case v’s.

The image in Figure 8 on page 27 provides an enlarged view of the URL in question. The deception perpetrated by this URL would escape all but the most rigorous scrutiny. Therein lies a problem: how many readers of e-mail pay sufficient attention to spelling in URLs to notice such a deception? How many readers of e-mail pay any attention at all to URLs?

As if the above forms of trickery were not bad enough, some phishing e-mails include JavaScript commands to spoof the URL that displays in the browser’s status bar when the user hovers his or her mouse over a hypertext link. In this way, the status bar will indicate that the URL points to TrustworthyBank.com, whereas...
in fact it actually points to, say, bankphishers.com. Likewise, phishers can exploit browser vulnerabilities to load content from one webpage while displaying the address of another. To see how this works in practice, simply follow these steps:

1. Open Internet Explorer.
2. Go to the Slashdot website: http://www.slashdot.org
3. Type the following into your browser:
   ```javascript
document.write("<iframe src='http://www.google.com' width='100%' height='100%'></iframe>\n");
```
4. Press enter. You will now see the Google home page in your browser, even though you are still logged on to the slashdot.org website.

Clicking on a hypertext link in a phishing e-mail to see which page loads is not an advisable URL identification strategy, since the link and/or page may have been crafted to spoof or cloak the URL. (Alternatively, the page may have been crafted to plant a virus on your computer, which is another good reason not to click on links in unsolicited e-mail messages.)

**Why Am I Being Targeted?**

Many phishing messages are sent out as spam. Since it is both inexpensive and easy for phishers to send millions of messages at a time, perpetrators can make money even if only a tiny percentage of users click on a link in a spoofed e-mail. Phishers also identify specific targets on social networking sites. The amount and quality of information that users disclose about themselves on social networking sites makes such sites particularly attractive pools within which to phish. Indeed, a social network phishing attack experiment conducted at Indiana University in April 2005 demonstrated a whopping “success” rate of 72%. Finally, phishing threats are not confined to e-mail; instant messaging (IM) is a major phishing vector as well.

**From Cause to Effect**

Research suggests that a considerable percentage of users have fallen victim to phishing attacks. An April 2004 Gartner study found that 19% of the survey participants (nearly 11 million U.S. adult Internet users) had clicked on a link in a phishing e-mail, and that 3% (approximately 1.78 million U.S. adult Internet users) had provided financial or personal information to phishers. These statistics confirm and reinforce the results of a U.S. Federal Trade Commission (FTC) survey conducted in March and April 2003:

- 1.5% of survey participants reported that in the previous year they had discovered that their personal information had been misused to open new credit accounts, take out new loans, or engage in other types of fraud.
- 2.4% of survey participants reported misuse of their information in the [previous] year that was limited to the misuse of one or more of their existing credit cards.
The purchase and sale of stolen personal data is fueling the emergence of an underground Internet economy.

The Underground Economy

In recognition of the fact that the purchase and sale of stolen personal data is fueling the emergence of an underground Internet economy, the eleventh volume of the Symantec Internet Security Threat Report, published in March 2007, includes a new item in its assessment, namely underground economy servers, which are “used by criminals and criminal organizations to sell stolen information, typically for subsequent use in identity theft.” During the second half of 2006, Symantec tracked the types of information that were exchanged via underground economy servers, and found that such information included “full identities, which typically involve government-issued identification numbers (such as social security numbers), bank account information (including passwords), personal information (such as date of birth), as well as identity verification information (such as a person’s mother’s maiden name).”

Perhaps even more disturbing than the types of information that are being exchanged on underground economy servers are the shockingly low advertised prices of such information. The aforementioned Symantec report notes that during the second half of 2006, U.S.-based credit cards with verification data were advertised at prices ranging from $1-$6 each, and complete identities (including U.S. bank account, credit card number, date of birth, and government-issued identity number) were advertised at a very modest $14-$18 each. The fact that these advertised underground prices are so low suggests that confidential personal information is both plentiful and easily obtained. The throwaway value of so-called confidential information should serve as a universal wake-up call about the importance of cyber security and of protecting confidential data.

From Detection to Prevention

Given the magnitude of the problem and the criticality of our confidential data, we must take all possible measures to protect ourselves from phishing e-mails and the people who send them. The most obvious strategy is to simply eliminate the phishing messages.

Figure 7

Figure 8

Phishing: How to Avoid Being Reeled in Continued

Unfortunately, as with spam, we cannot prevent unscrupulous individuals from sending us phishing e-mails. However, by following a few simple rules, we can virtually eliminate our risk of being reeled in by a phisher. Building on the recommended best practices discussed in the first article in this series (see “Spam—It Isn’t Just for Breakfast Any More,” in the April 2007 issue of The ATA Chronicle), the following strategies are suggested:

1. Be wary of generic account-related e-mails. As a general rule, legitimate e-mail messages sent by companies to their customers usually contain one or more pieces of personal information. For example, some companies address customers using their first and/or last names; others include partial account numbers (i.e., “accounts ending in XXXX”). By way of contrast, phishing messages generally do not contain personal information (the aforementioned “spear phishing” attacks being a notable exception). Therefore, if you receive an e-mail that contains no personal information, or which uses an impersonal greeting (such as “Dear PayPal Member” as in the screenshot in Figure 7), you should treat it with suspicion. Note, however, that the presence of personal information is not a guarantee of authenticity.

2. Do not click on links in unsolicited e-mail messages. If you receive an e-mail from a company with which you do business informing you that there is a security problem with your account and/or advising you that you need to “verify” your account information, contact the supposed sender company directly by phone to confirm that there is in fact a legitimate problem. Alternatively, open your web browser and type a trusted address for the company’s website (or select a legitimate, trusted address that you have previously bookmarked). Under no circumstances should you attempt to log on to a company’s site using a link provided in an e-mail message.

3. Do not provide confidential information that is requested via e-mail—ever. This advice should apply to any inquiry, whether by e-mail, fax, phone, SMS (text message), or any other medium. As a general rule, you should never share your user ID, password, credit card number, social security number, or other sensitive information with others unless: a) it is you who initiates the conversation; and b) you are certain that the person with whom you are speaking is an authorized representative of the company or organization, and that she or he requires the information for a legitimate purpose.

4. Beef up your security. Use a personal firewall in conjunction with a security software suite that offers anti-virus, anti-spam, anti-spyware, and anti-phishing features. Keep your operating system fully patched. Only conduct online financial transactions via secure web pages that use encryption. To tell if a page is secure, first verify that the URL begins with “https” instead of “http.” Then look for a closed padlock icon in the status bar of your browser (in the lower left corner of your screen). Click on the padlock to display the security certificate issued to the site. The name of the organization to which the security certificate has been issued should match the name of the site to which you are connected.

5. It you suspect fraud, err on the side of caution and act quickly. If you suspect that one or more of your accounts may have been compromised or that your identity may have been stolen, you should immediately log on to the Federal Trade Commission’s identity theft website, which contains instructions for filing complaints with the FTC and law enforcement as well as a list of steps that you can take to limit the damage.13

Conclusion

Phishing is a deceptive practice whereby criminals attempt to trick unsuspecting victims into revealing sensitive confidential information, which the perpetrators can then sell or use for fraudulent purposes. The scope and sophistication of phishing attacks have increased dramatically over the past several years, and this trend shows no sign...
of reversing itself. Our personal data is highly valuable, and we must treat it as such. A simple yet foolproof way to protect private information is to **never** respond to e-mail requests for such data, regardless of how realistic or seemingly plausible those requests may be.

**Notes**


2. According to Wikipedia, the substitution of the letters “ph” for “f” may reflect the influence of either phreaking or leetspeak; however, “[t]he popular theory that it is a portmanteau of *password harvesting* is an example of folk etymology.” From “Phishing.” Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/Phishing (March 19, 2007).


5. As of March 2007, this vulnerability does not appear to affect Firefox. However, Firefox exhibits other vulnerabilities. See Keizer, Gregg. “Firefox, IE7 Open to URL Spoof.” Computerworld (February 27, 2007). www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011939&intsrc=hm_list


10. Symantec, 30.


12. Symantec, 32.


**Additional Reading**


“[P]ractical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.” OnGuard Online (2007). http://onguardonline.gov/index.html

Stop-Phishing.com (The Anti-Phishing Group at Indiana University, 2007). www.indiana.edu/~phishing


Stop-Phishing.com (The Anti-Phishing Group at Indiana University, 2007). www.indiana.edu/~phishing