The Gentle Art of "Phishing"

Marilyn Dyrud, Oregon University of Technology

Abstract

"Give a man a fish," goes an old adage, "and you feed him for a day. Teach a man to fish, and you feed him for life." In Internet parlance, "Teach a man [person] to phish, and he can feast on caviar for the rest of his life." **Phishing** is a type of fraud unique to the Internet. All of us have probably received email from various credit card companies, banks, PayPal, or eBay alerting us to various activities regarding our accounts: break-in attempts, maintenance, or general "suspicious" activity. The message directs the user to a corporate website, which then requests sensitive information, including account number, PIN or ATM number, mother's maiden name, or social security number. While the websites look real, they are actually clever forgeries. Users who follow directions will later find their accounts vacuumed, their credit cards maxed out, and their identities stolen. This paper examines the different types of phishing, techniques used, and pedagogical applications.

Introduction

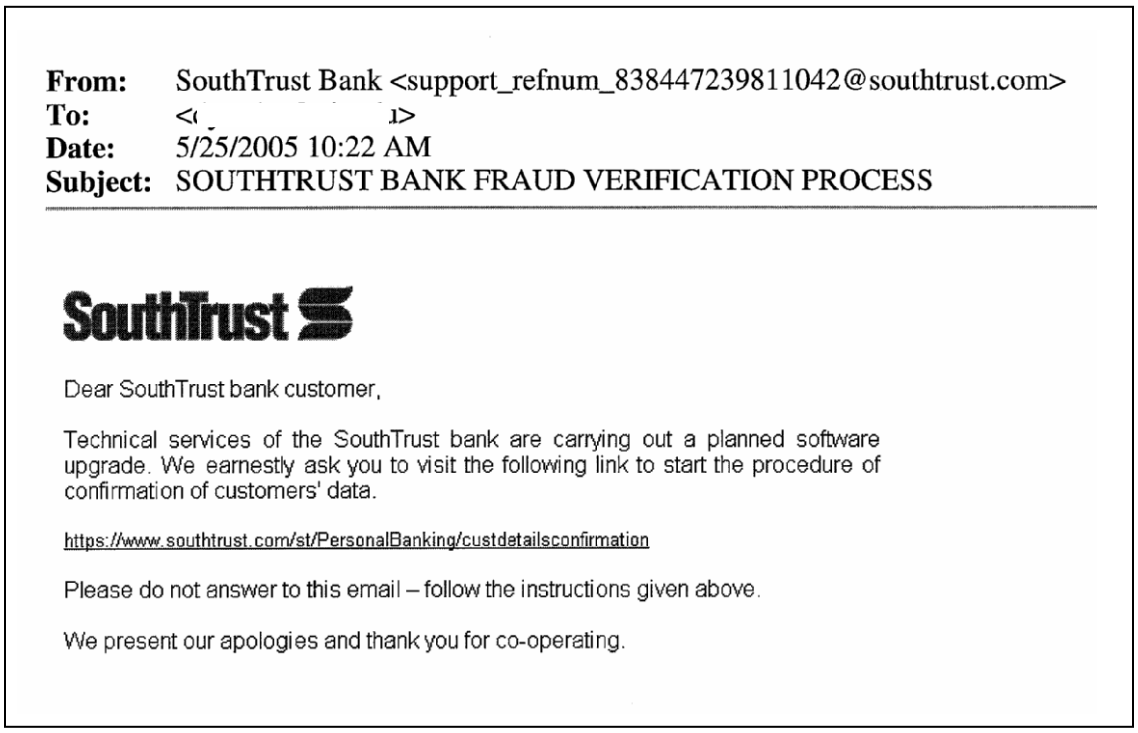
In *The Compleat Angler* (1668), Izaak Walton describes the art of fishing as a complex craft, "so like the mathematics that it can never be fully learnt; at least not so fully but that there will still be more new experiments left for the trial of other men that succeed us" (p. 224). Angling is a bucolic, contemplative sport, reflective of those who pursue it, "men of mild and sweet and peaceful spirits" (p. 234). Water itself has a mystical dimension; it is "nature's storehouse, in which she locks up her wonders" (p. 237). But beneath the placid surface lies danger: "there be monsters" (p. 232).

In the 350 years following Walton's meditative treatise, fishing has acquired a new face: in the deep waters of the Internet, there indeed be monsters, and the anglers who have succeeded Walton have transformed the serene into the sinister.

This paper examines the contemporary craft of Internet phishing, focusing on the different types, linguistic and technical deception techniques, and pedagogical suggestions. All examples, unless otherwise noted, are emails that the author has received. Since fraudulent messages comprise a significant portion of spam, as instructors we are obligated to alert our students so that, as professionals and consumers, they can avoid the tempting bait offered by Internet anglers.

Some Definitions

The term "phishing" was coined in 1996 (Olimann, 2004) and refers to email that directs users to counterfeit websites. The goal is to collect personal and financial information, which can then be used to make unauthorized purchases, steal identities, or sell sensitive information to identity theft rings. Figure 1 shows a typical phishing email.



From: SouthTrust Bank <support_refnum_838447239811042@southtrust.com>
To: <[redacted]>
Date: 5/25/2005 10:22 AM
Subject: SOUTHTRUST BANK FRAUD VERIFICATION PROCESS

SouthTrust

Dear SouthTrust bank customer,

Technical services of the SouthTrust bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation of customers' data.

https://www.southtrust.com/st/PersonalBanking/custdetailsconfirmation

Please do not answer to this email – follow the instructions given above.

We present our apologies and thank you for co-operating.

Figure 1. A phishing email

When users click on the link, they are directed to a site like the one in Figure 2. In addition to the information indicated, some sites will ask for more detailed data: bank account numbers, social security number, mother's maiden name, credit/debit card numbers, or the highly confidential CVV2 (the three-digit code on the back of credit cards). It is not unusual, however, for the link to be dead, as phishing requires a very tight timeline due to more effective detection tools. In fact, the average lifetime of a bogus website is a mere 5.5 days (MillerSmiles, October 2005).

Typically, phishers cast a wide net; they are part of an orchestrated international network. It is a very sophisticated operation, as Christopher Abad (2005) reports in his analysis of 3.9 million phishing emails gleaned from thousands of chat rooms and botnets. Abad concludes that phishing is "a thriving economic infrastructure," with as many as 250,000 concerted campaigns daily. "Phishing is," according to Ron Teixeira, director of the non-profit National Cyber Security Alliance, "probably the biggest threat consumers face on the Internet" (Sutel, 2006).

The numbers are astonishing. Phishing tends to occur in waves, and, according to a recent Federal Trade Commission estimate, in the US alone, traffic consists of 75-150 million messages a day, amounting to nearly $3 billion in annual losses to individuals and business (Heckman, 2006). Internationally, 2003 business losses totaled $32-39 billion (Drake, Oliver, & Koontz, 2004). About 70 percent of computer users who receive phishing emails believe that they are legitimate, as revealed by a joint AOL/National Cyber Security Alliance study (Kerr, 2005), and a recent AARP study conducted in Washington state notes that about half of survey respondents did not realize that legitimate financial institutions do not use email to ask clients for sensitive information (Heckman, 2006).

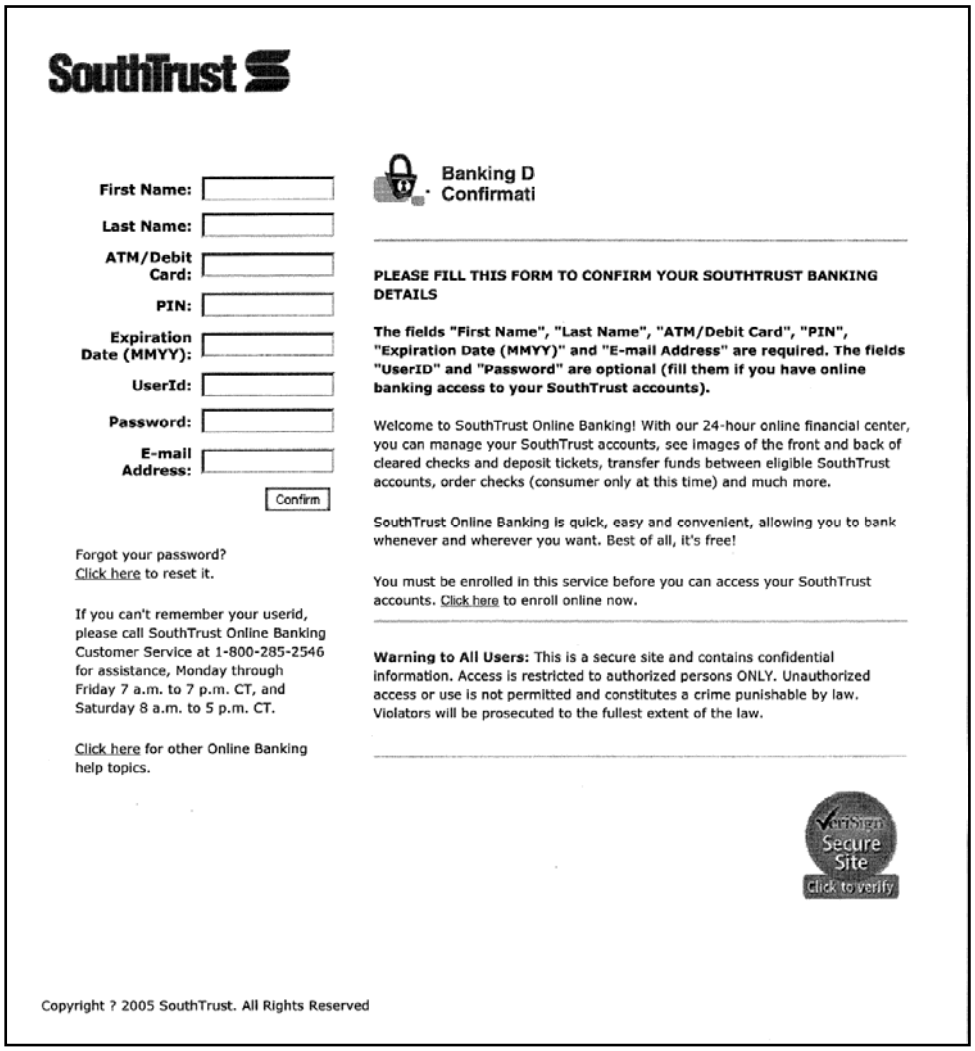


Figure 2. Phishing log-in page

Phishing is not a flash in the pan. Since its debut in 1996, the number and scope of attacks have increased to mind-boggling proportions. RSA Security is a firm that tracks global phishing ventures on a monthly basis; in June 2006, "almost 40 percent of all credit unions [in the US] were targeted," and international campaigns nearly doubled between April and June of 2006 (RSA, 2006). Even the IRS is not immune: phishers operating in 11 countries have hijacked IRS and Treasury Department logos to collect information for identity theft rings (IRS, 2006).

In the past few years, developing technology has allowed phishers to become more discerning regarding audience, resulting in two nuances on the theme.

Puddle Phishing

While many phishing attempts involve well-known Internet entities and financial giants, such as eBay, Amazon, PayPal, VISA, and Chase, puddle fishing refers to targeting smaller financial institutions such as the following:

- Alabama Credit Union
- Bangor Savings Bank (Maine)
- Bank of the West (California, specifically the East Bay area)
- Charter One Bank (Vermont)
- LaSalle Bank (Illinois, specifically Chicago)
- Montgomery County FCU (Maryland)
- People's Bank (Connecticut)

Phishers still need to refine their targeting techniques, however. I received emails from all of the above. Since I live on the West coast, my chance of having a bank account in Maryland or Vermont is virtually nil.

Spear Phishing

Spear phishing is new variation, emerging within the past year. Whereas general phishers trawl, netting all fish, spear phishers are more like scuba divers hunting a particular species. Spear phishing emails, from writers masquerading as the CEO or other power figures, target employees of one company in an attempt to steal passwords, which then allow them to plant Trojans that steal proprietary data. According to MillerSmiles, an anti-phishing news service based in the United Kingdom, the scam was first unveiled in June 2005 and "shows no sign of abatement" (MillerSmiles, August 2005).

Techniques of Deception

Phishers go to great lengths to deceive their intended victims, and some counterfeit websites are so faithful to the originals that only the most discerning eye can detect the difference. Phishers use both linguistic and technical ploys to steal sensitive data.

Linguistic Lures

It is the language of email, of course, that persuades receivers to part with sensitive information. Phishers play with language using the techniques explained below:

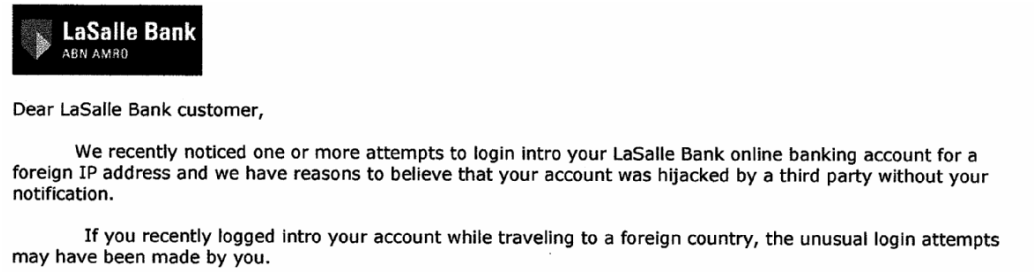
Subject lines and leads. Most phishing emails have subject lines that impart a sense of urgency:

- FRAUD IDENTIFICATION PROCESS (SouthTrust Bank)
- Please Confirm Your Details (Washington Mutual)
- Important fraud alert (Charter One Bank)
- Your account could be suspended! (eBay)
- Account suspension notice (PayPal)
- Please restore your account access (Horizon Credit Union)

- Attention! Several VISA Credit Card bases have been LOST!
- Fraud Prevention Measures (Bangor Savings Bank)

Given the news media's penchant for sensationalism—stories detailing, for example, the loss of millions of social security numbers from the Department of Veterans' Affairs database—email subject lines indicating fraud or loss of data may alarm the typical user. Even knowledgeable users have succumbed: Laurell Haapanen, a technical editor for a computer company, responded to a Washington Mutual email and later discovered that someone in Bucharest had "cleaned her out" (Heckman, 2006). Texan Timothy May learned of his error only when his credit card was denied at a business luncheon, much to his embarrassment. Soon thereafter, someone in Brooklyn used the stolen information to buy $5,000 worth of auto parts, and others in California bought a fleet of new Dell computers. The lesson learned? "I'll surf the Web and look at stuff, but I don't buy anything online anymore. It's just not worth it" (Krebs, 2004).

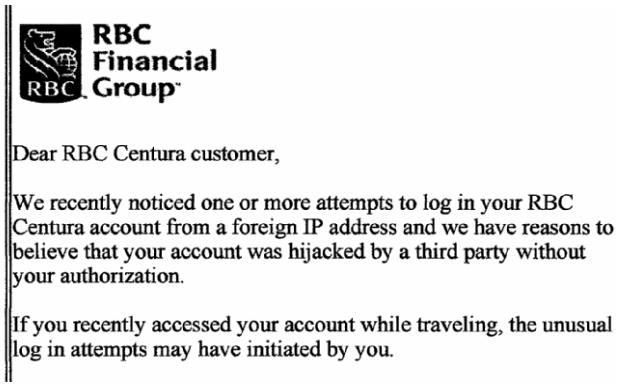
Opening paragraphs, or leads, may also sound the alarm bell, although an examination of several documents reveals that phishers tend to copy each other, as shown by these examples:


LaSalle Bank
ABN AMRO

Dear LaSalle Bank customer,

We recently noticed one or more attempts to login intro your LaSalle Bank online banking account for a foreign IP address and we have reasons to believe that your account was hijacked by a third party without your notification.

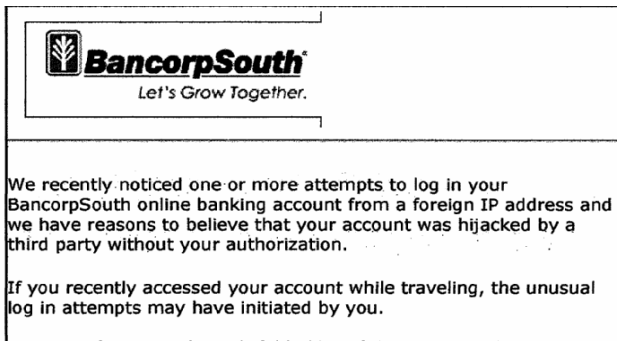
If you recently logged intro your account while traveling to a foreign country, the unusual login attempts may have been made by you.


RBC Financial Group

Dear RBC Centura customer,

We recently noticed one or more attempts to log in your RBC Centura account from a foreign IP address and we have reasons to believe that your account was hijacked by a third party without your authorization.

If you recently accessed your account while traveling, the unusual log in attempts may have initiated by you.


BancorpSouth
Let's Grow Together.

We recently noticed one or more attempts to log in your BancorpSouth online banking account from a foreign IP address and we have reasons to believe that your account was hijacked by a third party without your authorization.

If you recently accessed your account while traveling, the unusual log in attempts may have initiated by you.

Another strategy in leads is to offer false reassurances, as in the following from PayPal:

> PayPal is committed to maintaining a safe environment for its community of customers. To protect the security of your account, PayPal employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the PayPal system for unusual activity.

> We are contacting you to remind you that on July 21 2006 our Account Review Team identified some unusual activity in your account. In accordance with PayPal's User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved.

Some bogus websites give an illusion of reality by allowing users to link to the real organization's privacy statements or security policies, thereby enhancing the deception. Many also use the "https" citation ("s" stands for SSL, a data encryption program), and/or reproduce the secure verification logo.

Logical reasons. Phishing emails offer persuasive reasons for user action. Charter One Bank, for example, explains that routine software maintenance requires a profile update: "Technical services of the Charter One Bank are carrying out planned software upgrades. We earnestly ask you to visit the following link to start the procedure of confirmation of customers' data." At least five other banks, incidentally, use the identical wording and include this admonition: "This instruction has been sent to all bank customers and is obligatory to follow. Thank you for co-operating." Since even new users acknowledge the constant evolution of software and accompanying needs for replacement, this reason makes sense.

Other emails are more garden variety. A Bill Me Later notice informs me that my current billing statement is available for viewing, and an eBay notice alerts me that my bill for a 17" Dell monitor is still outstanding. I neither use Bill Me Later nor have an eBay account.

Some phishers use intimidation and threaten account closure; the following has been repeated in bank emails from all areas of the country: "This is your official notification from [bank name] that the service(s) listed below will be deactivate and deleted if not renewed immediately. Previous notifications have been sent to the Billing Contact assigned to this account. As the Primary Contact, you must renew the service(s) listed below or it will be deactivated and deleted." Recipients who do not currently indulge in online banking, the phishers wryly note, can enter their "SSN as Username and account number as Password."

Particularly at risk for this linguistic gambit are the elderly or technophobic, those whose computer use tends to be limited to email and holiday shopping sprees. Nancy Boyle, Racine, Wisconsin, responded to warnings from Bank One and eBay that her accounts were being suspended. After posting her social security number and her mother's maiden name, as requested, she discovered $1,800 missing from her bank account and an endless stream of credit card charges from Egypt (Krebs, 2004).

A final ploy offers prizes or money to users who follow the link: Chase Bank will send $20 to those completing a brief online survey, and in 2003, eBay was offering users the chance to win a Mercedes. The following year, "Shadow Crew," a fake company, even offered to send free child porn CDs!

Technical Decoys

In addition to linguistic lures, phishers are adept at manipulating technical details, by using JavaScript or ActiveX to achieve credible results. The following explains the most common techniques:

Addresses and URLs. Changes in the sender or "reply to" addresses are easy for scammers to implement and equally easy for users to overlook, as two eBay messages illustrate: eBay@eBays.com and eBay@ebay.com. In both cases, the changes, the addition of the "s" and the lower-cased "B," will direct the reply to bogus websites. The real address is eBay.com. Similarly, Bankcorpsouth instead of BankcorpSouth will send the user to a counterfeit site.

Another technique is even sneakier and essentially undetectable. In PayPal, the "l" is replaced with a capital "I." Using a sans serif font makes the replacement difficult to discern: **PayPal**, with the capital "I", or **PayPal**, with the "l" (see Drake et al., 2004, for many other examples).

The @ is a powerful symbol for phishers. Placed in a URL, it directs traffic to an alternate location, since some browsers, notably Internet Explorer, ignore information preceding the @. FraudWatch International (2003-6), a private company based in Melbourne, Australia, offers this example:

http://genuine-site.com-Verify83kcmdj30dk>Secure32902s;lkjasdfkljad@fraud-site.com

While the first part of the URL looks real, the user would actually end up at the site following the @: fraud-site.com. In fact, the longer the URL, the less attention users pay to it. To further disguise intentions, phishers may replace the @ with its hex equivalent, %40 (Drake et al., 2004; see also "How to Obscure," 2004, and Kay, 2004).

FraudWatch International collects examples of phishing techniques and publishes reports detailing website manipulation. Phishers use several techniques to manipulate URLs, such as replacing the address bar of a counterfeit site with the "real" one.

For example, they may add "hovering" text boxes, using JavaScript to disguise the bogus website address. Figure 3 shows this technique. While the URL looks real, it is actually placed over the phisher's address.

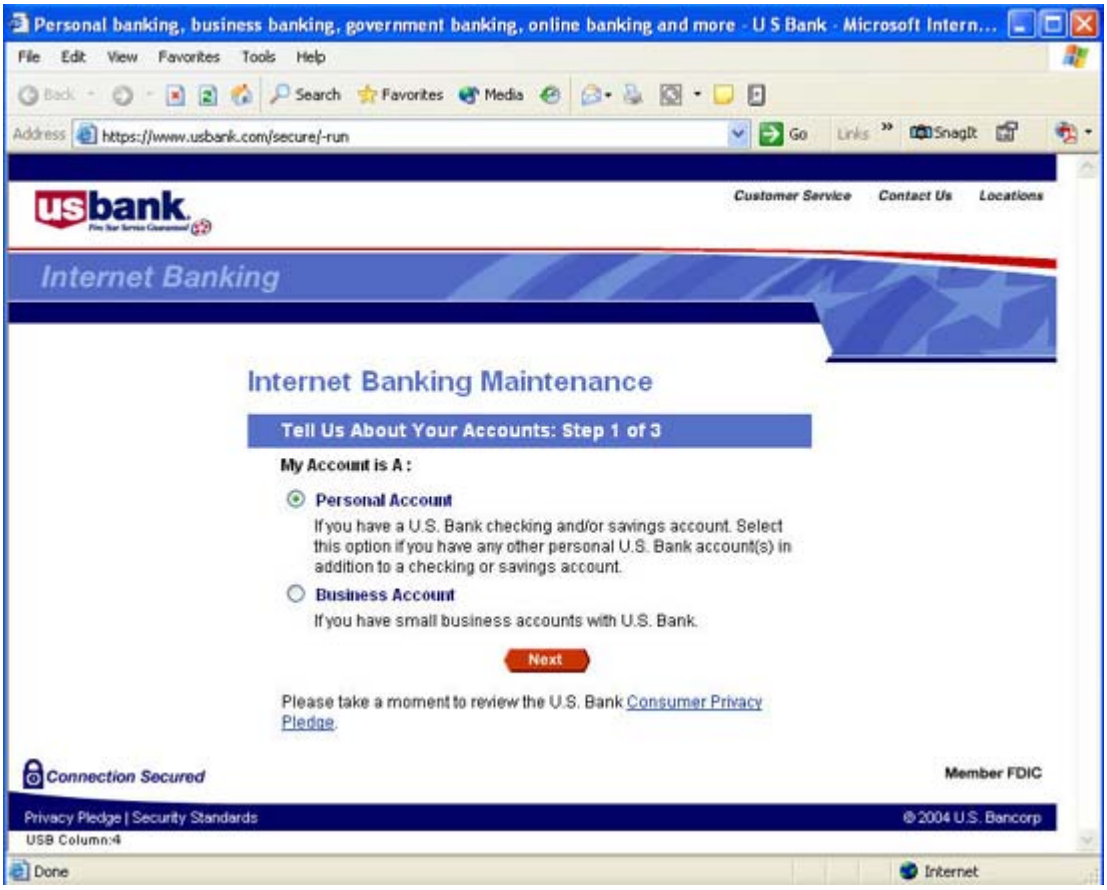


Figure 3. Hovering text box (FraudWatch International, 2003-6)

To detect phony addresses, open the Properties box, which will display the real URL, as shown in Figure 4.

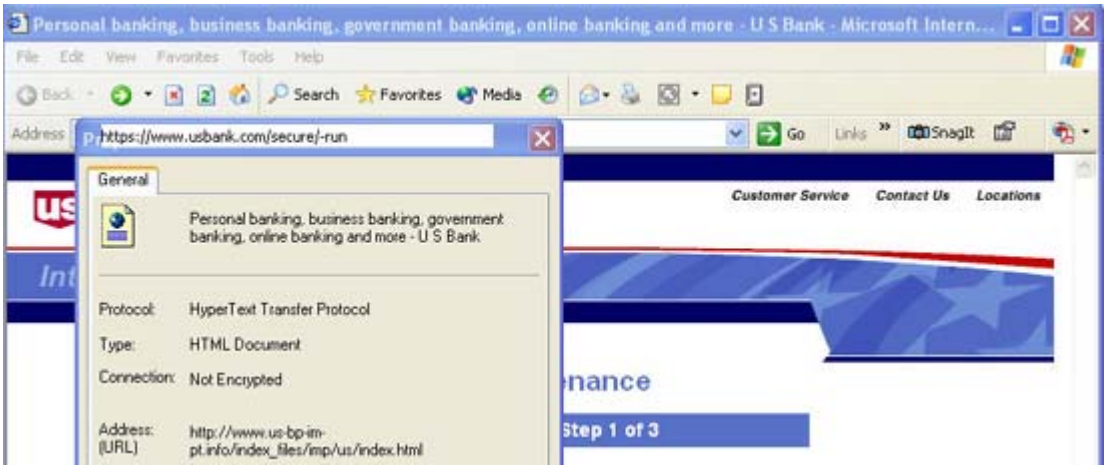


Figure 4. Properties box and real URL (FraudWatch International, 2003-6)

Less technically adept phishers make few or no attempts to disguise their deception, and simply truncating a URL will take the user to the originating site, often located in Europe or Asia. For example, clicking on the link in an April 7, 2006, PayPal update notice purporting to "reduce the instance of fraud" takes the user to a log-in page; the status bar displays a distinctly different address, http://www.soribook.or.kr/.paypal.comlus/cgi-binlindex.php, than the email "from" line: service@paypal.com. Truncating the address to www.soribrook.or.kr leads the user to a Korean site (Figure 5).

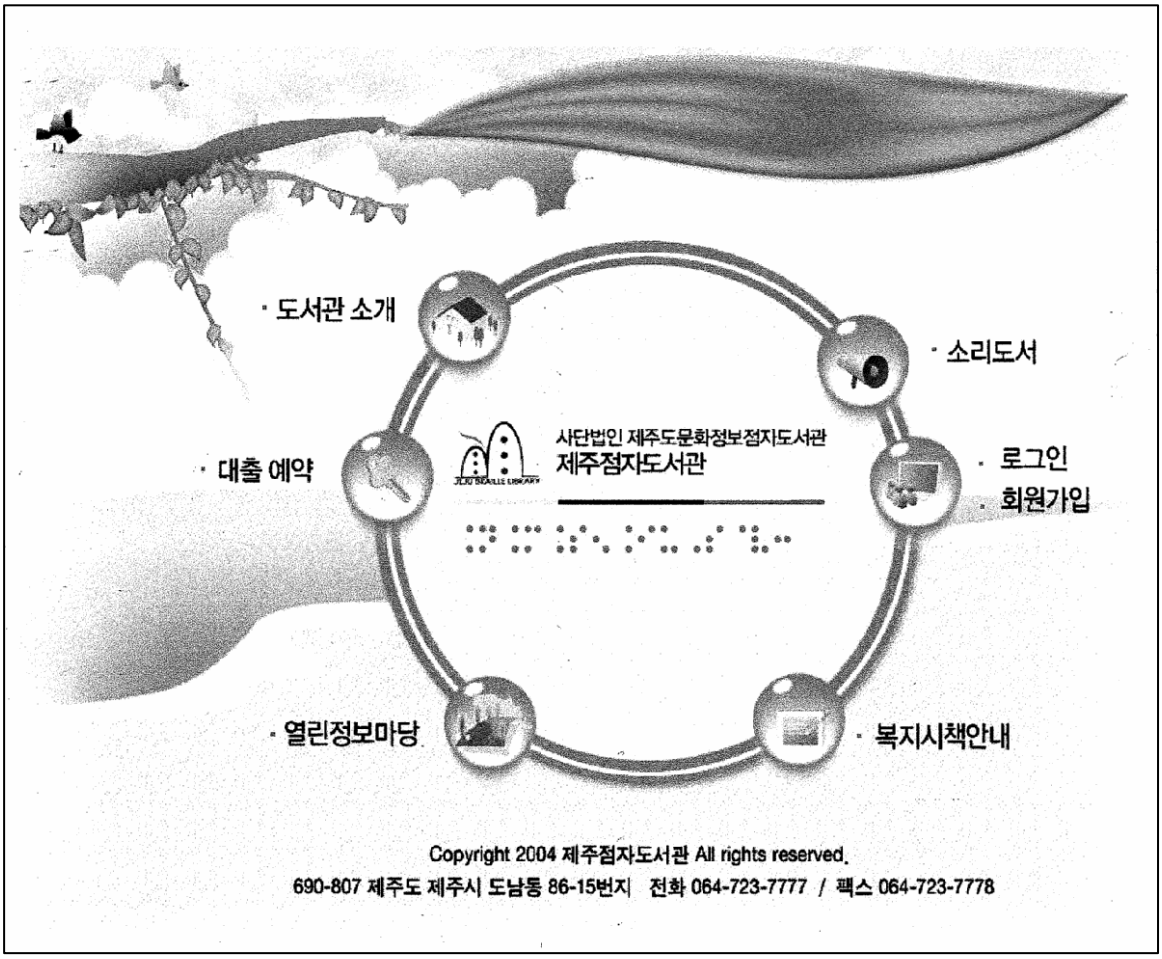
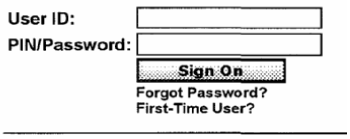


Figure 5. Originating website for PayPal phishing attempt

Pop-ups. Producing a counterfeit website is time-consuming and requires considerable programming expertise. Some phishers, therefore, resort to using real corporate websites and simply add pop-ups rather than reproducing home and log-in pages. Clicking on the link in a recent PNC Bank notice yields this simple pop-up, rather than a counterfeit log-in page.



Whole site counterfeiting. Phishers with a programming background can create convincing replicas of real sites, as shown in Figure 6. Figure 7 is the real PayPal page, downloaded on the same day as the phishing example. On the surface, they look identical. However, more careful scrutiny reveals that the counterfeit page is missing several items, most notably the links to other countries and PayPal-related sites, the secure verification symbol, and, most significantly, the SSL certificate link. SSL is an encryption program intended to ensure that information entered on a company website cannot be transmitted to third-party users, and the certificate verifies the exercise of "due diligence" in protecting sensitive information (Krebs, 2006).

Other variations include the copyright dates, 1999-2005 for the fake site and 1999-2006 for the real one, and membership citations, 71 million for the phishing site and 96.2 million for the real site. The slight differences suggest that phishers are either using dated information or that their site was created in 2005 and has been recycled for the past year.

Many users do not see these small discrepancies, as Delores Hanes, a 77-year-old from Vancouver, Washington, discovered. After responding to a PayPal notice, she realized her error: charges starting accruing to her checking account, Western Union sent an electronic payment transfer to a German address, and someone opened up an AOL account in her name. "It had the PayPal pictures all over it," she said. "On the surface at least it looked like everything else I'd seen from them" (Krebs, 2004).

The problem is persistent enough to prompt MasterCard and other credit giants to "aggressively combat" such schemes ("MasterCard," 2004) by partnering with firms such as NameProtect, a provider of detection technology. As a MasterCard senior vice-president stated, "We are confronting identity theft head-on by taking the flight directly to where payment card scams breed and spread." But that was two years ago, and the problem has hardly been solved; indeed, more phishing scams now exist than ever before. Between December 2005 and January 2006, unique phishing sites increased by 2,600, according to data collected by the Anti-Phishing Work Group (2005, 2006).

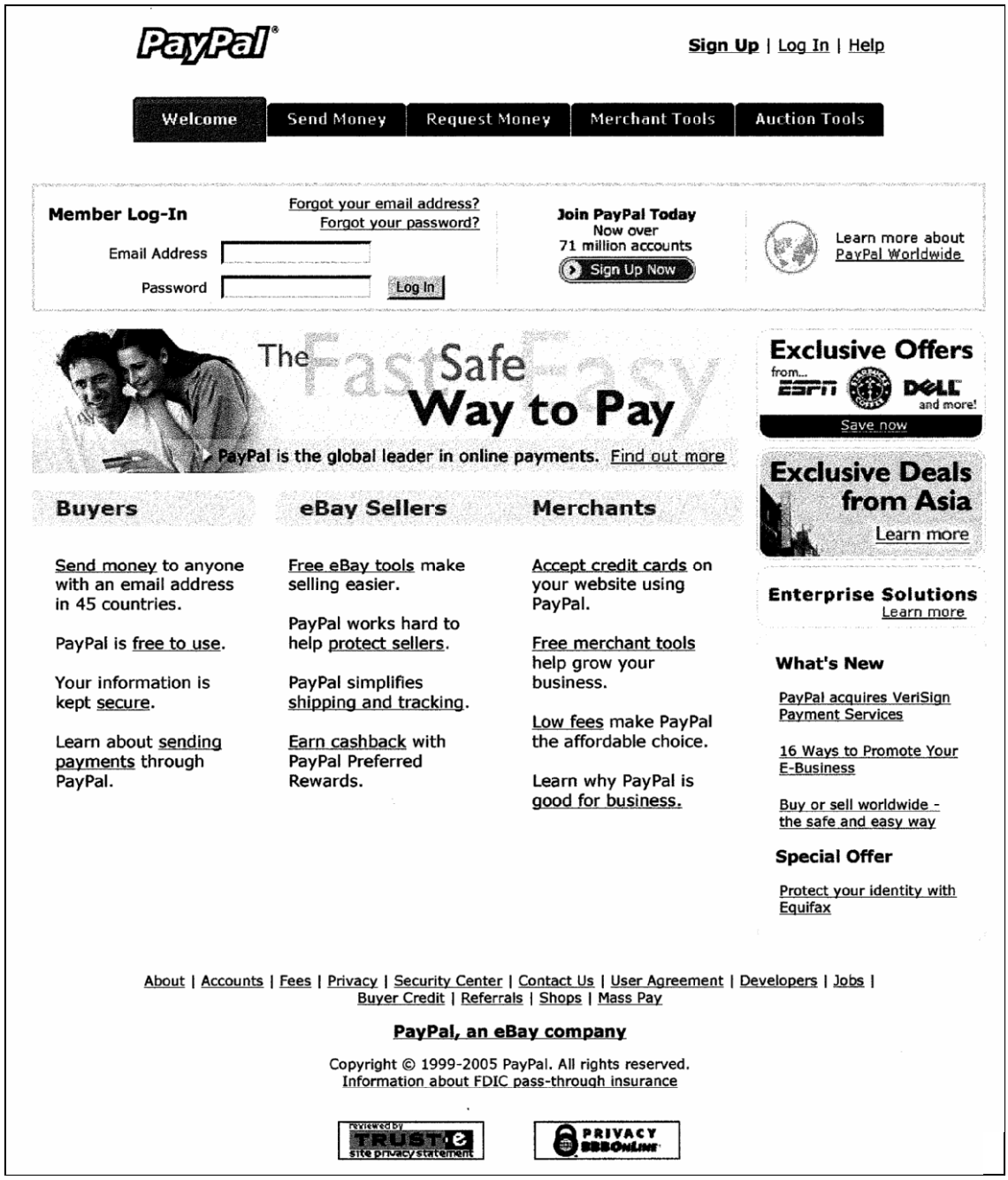


Figure 6. Phishing PayPal log-in page

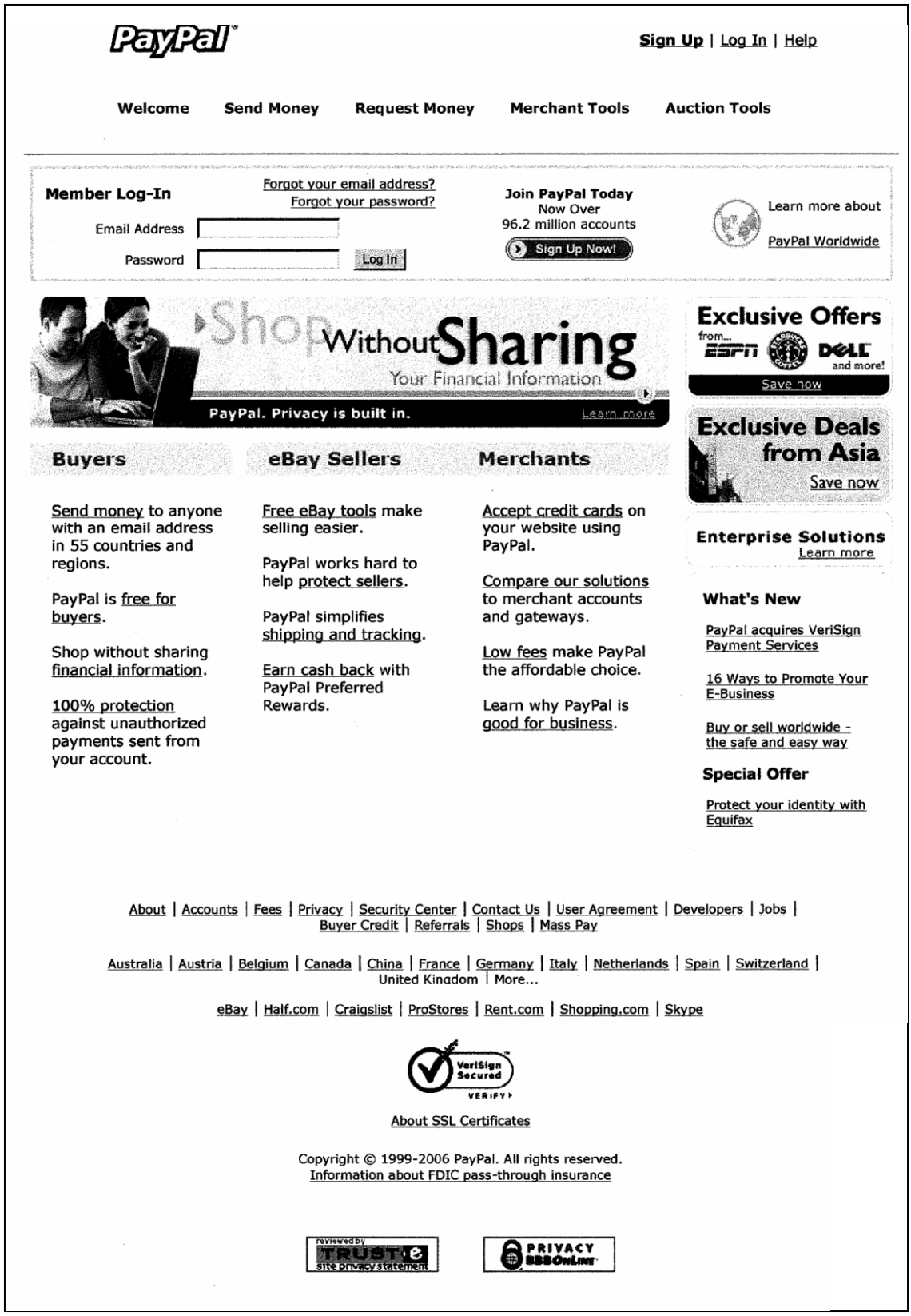


Figure 7. Real PayPal log-in page

Trojans. Perhaps the most insidious technique used is planting undetectable "keylogger" Trojans or worms in the log-in link (Olimann, 2004). They can also be hidden in email attachments or shared files. Once installed, they track keystrokes and allow thieves to steal sensitive data when users log-on to particular sites, such as banks or credit card accounts. A 2005 estimate indicates the existence of about 6,000 different keylogger programs, with as many as 9.9 million affected computers in the United States alone (Zeller, 2006).

Horror stories abound. Joe Lopez of Miami, for example, lost $90,000 after a keylogger Trojan transferred the money from his business account to Latvia, and 55 members of a Brazilian keylogging gang, which collected $4.7 million from 200 accounts, were arrested last February (Zeller, 2006).

Classroom Applications

Phishing lends itself to classroom examination, particularly in classes that explore the rich—and rapidly expanding—area of Internet fraud. Instructors first need to acquaint themselves with the current scams and collect plenty of examples to share with their classes.

Instructional Resources

With the specter of data-snatching malware looming in the background, instructors may be reluctant to link to bogus websites. Fortunately, several watchdog groups track phishing attempts. The Anti-Phishing Working Group (anti-phishing.org) is a consortium of nearly 60 businesses and universities; it maintains a two-year archive that not only displays phishing emails but offers explanations as to frequency and, occasionally, commentaries on effectiveness. MillerSmiles (millersmiles.co.uk) keeps a daily log of phishing scams on its homepage, archives emails from some 395 companies, internationally, and ranks them as to severity of threat. And PhishRegistry (www.phishregistry.org/), created for US businesses and financial institutions, graphically displays monthly phishing activity and a listing of phishing emails. Unlike the other two sites, however, PhishRegistry does not reproduce the original messages.

Activities

Creative instructors can develop a myriad of activities centering on phishing. Listed below are some that students in my Business Correspondence and Electronic Communication & Society classes have found interesting and enlightening.

In The Classroom. If time is at a premium, consider some short, inclass exercises involving language analysis and subject line effectiveness. Many phishing emails display ESL characteristics similar to Nigerian fraud letters. Phrases such as "we earnestly ask" are tip-offs to non-native origins. Some entire emails are laughably non-professional, as in Figure 8, which purports to be from VISA:

From: VISA Service [VisaCard@visa.com]
Sent: Thursday, February 23, 2006 11:49 PM
To:
Subject: Attention! Several VISA Credit Card bases have been LOST!

Good afternoon, unfortunately some processings have been cracked by hackers, so a new secure code to protect your data has been introduced by Visa. You should check your card balance and in case of suspicious transactions immediately contact your card issuing bank. If you don't see any suspicious transactions, it doesn't mean that the card is not lost and cannot be used. Probably, your card issuers have not updated information yet. That is why we strongly recommend you to visit our website and update your profile, otherwise we cannot guarantee stolen money repayment. Thank you for your attention. Click here and update your profile.

Figure 8. Ineffective VISA phishing example

Other emails include misspellings ("apriciate" instead of "appreciate," "you're" instead of "your," "fallow instead of "follow") that indicate non-professional origins, as do made-up words ("securise").

Looking at subject lines/signatures is also a short activity that students seem to enjoy. Students can examine a number of subject lines for effectiveness, such as these:

- [Bank name] Notice
- Important information regarding your account
- Unlock your Account
- Your Account Was Hijacked!
- Online banking records confirmation
- Important Notice!

Ask students to consider which email, given the subject line, they would open and which point to a phishing attempt. Are haphazard capitalizations or use of exclamation points effective?

Looking at the signature lines of several emails is also illuminating. Some are generically "team," such as "The PayPal Team," "The eBay Team," "The Sky Bank Team," and "The WAMU Security Department Team." In reality, banks never use such signatures. The use of "team" is a dead giveaway that the email is bogus. Some even use the names of persons, such as "Thank you, sincerely, Tricia Doyle, Customer Services." In examining several emails, it appears that Tricia is a very busy person, serving as the customer services representative for BankcorpSouth, USAA Federal Savings Bank, Flagstar Bank, and, undoubtedly, a number of others. John Hartman is equally popular, serving at Sun National Bank, Chase, and Alabama Credit Union. Most users, however, would not notice the repetition, since they are looking at their email in isolation; they are not collecting and analyzing a number of phishing attempts.

In The Computer lab. Instructors who teach in a lab setting can engage in a number of online activities. By taking a "phishing IQ test," students can discover what they know about this type of fraud. MailFrontier (2004) has a 10-item quiz that reproduces original emails; students indicate whether they think the site either legitimate or fraudulent, and, after finishing, they can

check their answers. In addition to providing the correct responses, the answer page also gives reasons, such as the ones shown in Figure 9. The site also includes statistics and a link to a very cute and useful *Field Guide to Phishing* (MailFrontier, 2005).

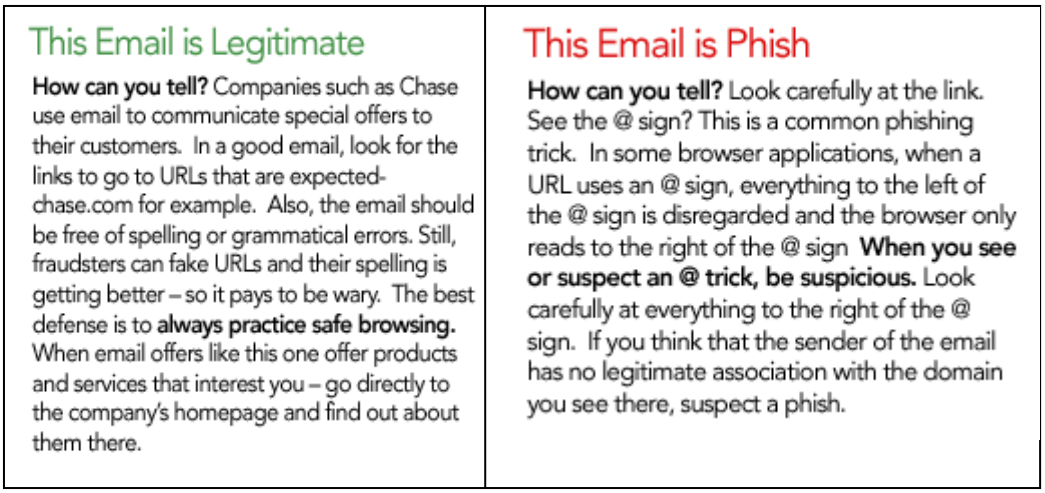


Figure 9. Examples from MailFrontier IQ test

"Phind a phisher" is an enlightening activity that involves ferreting out the real culprits hiding behind fake URLs. Using either the Properties box or truncating the address can take students all over the world. In my own virtual travels, I've discovered originating sites on every continent except Antarctica.

Research. Instructors who teach classes with a critical thinking component can have students research a number of issues concerning Internet fraud:

- Privacy
- Data protection
- Identity theft
- Legislation addressing Internet fraud
- Detection technology
- Effect of the Internet on business communication
- Case studies involving phishing or other types of fraud
- The future of phishing (instant messaging, pharming)

Any of these topics would make an interesting research project and afford students an opportunity to examine how the Internet is changing both personal and professional communication and redefining who we are.

Having students examine professional codes of ethics is also an enlightening exercise. While phishers are not considered to be professionals, their actions are not only unethical but illegal as well. Looking at codes is a way of acquainting students with issues in various professional fields. Appropriate codes for Internet fraud include the Software Engineering Code of Ethics and Professional Practice, Association of Computer Machinery (all available from the Online Ethics Center for Engineering and Science, onlineethics.org/codes/index.html), and the Association of Information Technology Professionals Code of Ethics (available from the AITP, www.aitp.org/organization/about/ethics/ethics.jsp). The Center for Study of Ethics in the Professions, at Illinois Institute of Technology (ethics.iit.edu/) maintains a library of codes, searchable by subject area.

Conclusions

In *The Road Ahead* (1995), Bill Gates paints a remarkably rosy picture of the future of computing technology:

> The global information market will be huge and will combine all the various ways human goods, services, and ideas are exchanged. On a practical level, this will give you broader choices about most things, including how your earn and invest, what you buy and how much you pay for it, who your friends are and how you spend your time with them, and where and how securely you and your family live. Your workplace and your idea of what it means to be "educated" will be transformed, perhaps almost beyond recognition. Your sense of identity, of who you are and where you belong, may open up considerably (pp. 6-7).

In the decade since, all of these things have materialized. However, what Gates didn't predict is the fact that the computer revolution has also allowed for significant changes in criminal behavior. Gates saw computerized information as "totally private": "As long as you protect the password, the information stored on your computer can be held under the strongest lock and key that has ever existed. This allows for the greatest degree of information privacy any individual has ever had" (p. 270).

Ignoring the irony that Microsoft's Internet Explorer offers many holes for adept phishers, the privacy forecast by Gates simply has not materialized. Quite the contrary: computers offer malicious phishers a cornucopia of private information, which they gleefully harvest, violating users' sense of trust. Those who have been phished have been, metaphorically speaking, electronically raped, and they experience feelings of vulnerability and powerlessness.

If for no other reason, exploring Internet fraud in class will help our students be smarter users, both personally and professionally. With more informed users, perhaps then another of Gates' predictions will come true: that computers will function as "symbolic mediators that amplify the intellect" (p. 5).

References

Abad, C. (2005). The economy of phishing: A survey of the operations of the phishing market. *First Monday, 10*(9). Retrieved March 22, 2006, from http://www.firstmonday.org/issues/issue10_9/abad

Anti-Phishing Work Group. (2005, December). Phishing activity trends report. Retrieved April 30, 2006, from http://www.antiphishing.org/reports/apwg_report_DEC2005_FINAL.pdf

Anti-Phishing Work Group. (2006, January). Phishing activity trends report. Retrieved April 30, 2006, from http://www.antiphishing.org/reports/apwg_report_jan_2006.pdf

Drake, C. E., Oliver, J. J., & Koontz, E. J. (2004). Anatomy of a phishing email. *Proceedings of the First Conference on Email and Anti-Spam*. Retrieved July 10, 2006, from www.ceas.cc/papers-2004/114.pdf

FraudWatch International. (2003-6). *Phishing web site methods*. Retrieved March 22, 2006, from http://www.fraudwatchinternational.com/phishing-fraud/phishing-web-site-methods/

Gates, B. (1995). *The road ahead*. New York: Viking.

Heckman, C. (2006, May 1). Phishing finds victims even among savvy computer users. *Seattle Post-Intelligencer*. Retrieved July 24, 2006, from http://seattlepi.nwsource.com/lifestyle/268403_phishing01.html

How to obscure any URL: How spammers and scammers hide and confuse. (2002, January 13). Retrieved July 28, 2006, from http://www.pc-help.org/obscure.htm

IRS: "Phishing" ID theft scams on rise. (2006, March 13). *CBS News*. Retrieved July 27, 2006, from http://www.cbsnews.com/stories/2006/03/13/tech/main1397673.shtml

Kay, R. (2004, January 19). Phishing. *Computerworld*. Retrieved March 20, 2006, from http://www.computerworld.com/securitytopics/security/story/0,10801,89096,00.html

Kerr, J, C. (2005, December 7). Study: Phishing spam hits 1 in 4. *CBS News*. Retrieved July 27, 2006, from http://www.cbsnews.com/stories/2005/12/07/tech/main1103342.shtml

Krebs, B. (2004, November 18). Phishing schemes scar victims. *The Washington Post*. Retrieved March 15, 2006, from http://www.washingtonpost.com/ac2/wp-dyn/A59349-2004Nov18?language=printer

Krebs, B. (2006, February 13). Security Fix: The new face of phishing. *Washingtonpost.com*. Retrieved March 22, 2006, from http://blog.washingtonpost.com/securityfix/2006/02/the_new_face_of_phishing_1.html

MailFrontier. (2004). *Mail phishing IQ test II*. Retrieved April 4, 2006, from http://survey.mailfrontier.com/survey/quiztest.html

MailFrontier. (2005). MailFrontier field guide to phishing. Retrieved March 22, 2006, from http://www.mailfrontier.com/docs/field_guide.pdf

MasterCard tackles phishing scammers. (2004, June 22). *Digital Trends*. Retrieved April 4, 2006, from http://news.digitaltrends.com/article4405.html

MillerSmiles News. (2005, August 21). *Spear-phishing phenomenon*. Retrieved July 28, 2006, from http://news.millersmiles.co.uk/article/0056

MillerSmiles News. (2005, October 24). *Phishing—A tougher art*. Retrieved July 28, 2006, from http://news.millersmiles.co.uk/article/0061

Olimann, G. (2004, September). *The phishing guide: Understanding and preventing phishing attacks*. Retrieved March 3, 2006, from http://www.ngssoftware.com/papers/NISR-WP-Phishing.pdf

RSA Consumer Solutions. (2006, June). *Monthly online fraud intelligence report*. Retrieved July 2, 2006, from http://www.rsasecurity.com/solutions/consumer_authentication/intelreport/RSA%20Online%20Fraud%20Intel%20Report%20-%20June%202006.pdf

Sutel, S. (2006, May 14). Be cautious of "phishing" email scams. *Herald and News*, D3.

Walton, I. (1668; rpt. 1963). The compleat angler. In A. M. Witherspoon and F. J. Warnke (Eds.). *Seventeenth-century prose and poetry* (2nd ed.; pp. 222-50). New York: Harcourt, Brace & World.

Zeller, T., Jr. (2006, February 27). Cyberthieves silently copy your passwords as you type. *The New York Times*. Retrieved March 20, 2006, from http://www.nytimes.com/2006/02/27/technology/27hack.html?pagewanted=2&ei=5087&en=c3573b41b87a8552&ex=1156827600&excamp=GGTEphishing