

Something Smells Phishy

Crooks 'Phish' for Victims Via Email

By LIBBY CARTY MCNAMEE

The SunTrust Bank customer—let's call her Angela—recently received an email, complete with the bank's familiar logo, warning her about the recent surge of "phishing" attacks against the bank. In order to bolster security and combat these attacks, the email demanded that she click on an attached link and re-enter her social security number, various account numbers, address, and password. If she did not comply within forty-eight hours, the security department would terminate the accounts she had held for years.

Hmmmn... Sound fishy? Shouldn't Angela's bank have already had that information on file?

Of course it should have. Angela had nearly become victim to the very scam the email was supposedly warning her about: phishing.

This rampant cyber-crime, which the FBI has called the "hottest, and most troubling, new scam on the Internet," occurs when an online thief sends spam (unwanted email solicitations) to "phish" (or fish) for personal information: passwords, user IDs, credit card numbers, account and PIN numbers, social-security numbers, and so on. Once armed with this data, the phisher can then illicitly withdraw money and make online purchases—or even engage in identity theft by opening up credit cards in the victim's name without her knowledge and having bills sent to a designated address.

The bait for phishing is a seemingly official email, just like the one Angela received, that *looks* as if the victim's bank or financial institution has sent it. In the body of the email, the phisher requires the recipient to "re-enter" or "validate" personal account information for some reason—for instance, to access a newly updated system.

In reality, the email originated from the phisher's own website, a phony look-alike of the bank's *real* site with the same trusted trademarked graphics. Although not common knowledge, it is remarkably easy for phishers to replicate information from a legitimate business website and use it on their own fraudulent one. According to the Anti-Phishing Working Group, phishers have been able to convince some five percent of recipients of their bulk fraudulent emails to respond and thus divulge personal data by hijacking the trusted brands of well-known banks, online retailers, and credit-card companies.

Internet Identity, a consulting firm specializing in anti-phishing defenses, estimates that the average impact per person is \$92,000. Since there are usually hundreds of individual victims per incident, the total loss is often well over ten million dollars. The victimized companies, not the consumer, usually end up bearing the

loss. Gartner Inc. estimates that phishing schemes alone have cost banks over \$1.3 billion.

Other common phishing scenarios deal with similarly urgent false statements as bait, such as a claim that someone has used a person's Visa card without her knowledge or a fabricated notification that she has won a prize or inherited some money. The online auction house eBay is a frequently targeted business; both buyers and sellers have been victimized by phishing.

Unfortunately, Richmond businesses have not been immune from this accelerating cyber-crime. Capital One's website alerts its cus-

tomers about potential phishing attacks, warning "beware of fraudulent emails." SunTrust offers extensive anti-phishing information on its website as well. SunTrust industry spokesman Hugh Suhr explained, "Unfortunately this is an industry-wide problem in which everyone is a target."

Although it is extremely difficult to apprehend phishers because of Internet anonymity and overseas locations, some federal and state laws criminalize phishing with substantial penalties. Last February, the Virginia Legislature approved anti-phishing legislation introduced by former Attorney General Jerry Kilgore. **EP**