

LAW and ORDER

Email Security Concerns

by Kevin Gordon

Take a minute and think how often you use the Internet in both your working life and personal life. While the Internet has many uses and benefits, the aspect of the Net that the majority of us use is e-mail. Hard to imagine that e-mail and the Net itself as we know it did not come into use until about 14 years ago. Most police departments did not begin using the Net for official purposes until just the last three to five years. In just a few short years, e-mail has become such a part of our lives it seems like it has been with us forever.

We are all aware of the variety of threats to our computer and the data that lies within, but it is easy to forget that in our busy daily lives. Coupled with this familiarity, it can cause us to disregard the security concerns. Like many of you, even with my junk filters on I spend as much time deleting spam e-mails as I do reading the good ones.

Just when I became accustomed to the phishing e-mails announcing sexual enhancements both in drug form and personal implants, cheaper mortgages and millions waiting for me in Nigeria, now I must try to sift through e-mails that are not as obvious as previous spam but may contain even more threats than in the past. The new e-mails directed to selected users are called spearphishing. You have to love the jargon of the Net!

Be honest, how often have you opened an e-mail that was suspicious but your curiosity got the best of you. You just had to look! Attackers realize that and often take advantage of such curiosity by using deceptively named links. The social engineer collects just enough easily available information to create an e-mail that you take as legitimate.

Fortunately most such e-mails are not attacks but efforts to sell a product. But it only takes one actual "attack" to cause serious issues for your agency. If you have fallen victim to that, it is time to change that behavior. The e-mail threats are increasing, not decreasing, and remember, while firewalls may block direct attacks, e-mail provides a very vulnerable route into your agency or home computer.

A recent unclassified United States Department of Homeland Security Joint Information Bulletin provides that experts believe the biggest security vulnerability facing computer users and networks today is e-mail with concealed Trojan Horse software. In non-technology terms, the best deadbolts on your doors are useless if not locked. By use of such tainted e-mails, the sender has used an unwilling and often unwitting accomplice, the computer user. On the reverse, the most important line of defense against such attacks is the user.

You may be very familiar with what to watch for but maybe other officers or even family members are not as aware, so let them know to look for deceptive e-mail subject lines, e-mails that claim to originate from a family member or coworker or friend that is misspelled, or anything different from a normal e-mail from them.

Watch e-mails from folks you never had contact with or e-mails that seem to be part of an ongoing conversation that you never had, or with attachments that you are not expecting. Remind others that such e-mails don't need to include an obvious attachment but may have embedded links to what appears to be an innocent Web site which in reality downloads a malicious code.

So how do you and your other officers stay aware of such threats? Many Web sites provide updated security information but don't visit them once or even occasionally, visit them often! Put on your "to do" calendar to read the latest security information on a regular schedule.

Don't forget to inform the clerical help (who are often overlooked and usually spend more time online

than others) of security info items. And remember the folks down the hall in the public works or clerks office who are networked to your system for the purpose of in-house e-mail—keep them informed also!

Here are a few suggested sites to visit:

- CERT Coordination Center at <http://www.cert.org>.
- The United States Computer Emergency Readiness Team at <http://www.us-cert.gov> has excellent publications for download and many links to other good sites.
- The National Vulnerability Database at <http://www.nvd.nist.gov>.
- The US Dept. of Homeland Security Ready site at <http://www.ready.gov>.
- The Cyber Science Laboratory Resource Center at <http://www.cybersciencelab.com/>.

Kevin Gordon spent 25 years in law enforcement and retired as a chief of police. He can be reached at Kevin@KGordon.com.

This article was printed in Law and Order Magazine, April 2006.