## Dirty Dozen Clues to Avoid Phishing Attempts

*Steven Lovaas, Colorado State University, rev. 2016*

Phishing (no, it's not a very good name, but someone published it and it stuck) is a term for the use of "social engineering" tactics in email. The attacker tries to exploit the trust with which people usually approach messages from friends and known business associates. We're not necessarily talking spam here…most garden-variety spam is obvious by now (think Viagra). For phishing, we're talking deception, which means a less-obvious, possibly well-crafted forgery of what might seem like a legitimate message. Here's a list of some things that ought to make you go "hmm…" especially if more than one or two of them is present:

1. Impersonal greeting (dear webmail user)
2. Inappropriate "from" address (visually obvious - not from your organization at all)
3. Mismatched "from" address (less obvious - friendly name doesn't match the real @address)
4. Mismatched URLs in the body (even less obvious - mouse-over doesn't match the display, or if the email client is not HTML-enabled, the description of the link doesn't match the full URL)
5. Dire warnings. No legitimate organization would actually send an email telling a user that their account will expire permanently in 24 hours if they don't click here!
6. "Too-good-to-be-true" offers that expire very quickly. Think Dire Warning in reverse: nobody from Nigeria is going to send you any money.
7. Request in the email for username and password, or for sensitive personal or financial information. Typically, in the rare case that a legitimate organization actually needs you to do this, they'll notify you in advance that such a request is coming. Even so, it's better to tell users to go to the organization's main web page and follow the link to "Reset your password", rather than including a link to the actual re-set page in the email body itself. Here's a case where user-friendly and helpful tactics actually should make us more suspicious. Bummer.
8. Lame excuses by large organizations. Do you think that Amazon really needs your help in rebuilding or confirming its customer contact database? Have you ever had a retailer purge you from a catalog mailing list because you didn't return an email?
9. INSTRUCTIONS IN ALL CAPS (see #5, dire warnings).
10. Email from a part of your organization that doesn't actually exist by that name, or with that email (if you don't have something called a Helpdesk, but most of your IT messages come from Central IT Support... what should you do with an email that claims to be from helpdesk@yourorganization.com?) - this won't stop so-called "spearphishing," which is targeted specifically at your organization with good information-gathering in advance, but it'll help you notice the bulk of phishing attacks, which are still sent to big lists with fairly generic information.
11. Email from a commercial organization you don't do business with. If you don't have a Capital One credit card, why should you respond to re-set your account information?
12. The little voice inside your head - it's pretty good at noticing things that don't quite feel right. Pay attention!

Of course, sometimes legitimate emails will look a little suspicious. Not everyone is aware of all the clues they include in their communications .Even those of us who do pay attention to these things sometimes slip up. Ultimately, it's about being aware of what you're being asked to do, rather than just automatically trusting everything your computer tells you!

As always, if you have questions about this list or feel unsure about something you're being asked to do via email, don't hesitate to contact me.

Steven Lovaas
IT Security Manager
Colorado State University
Steven.lovaas@colostate.edu
(970) 297-3707