Sept 19,2014 Release #284

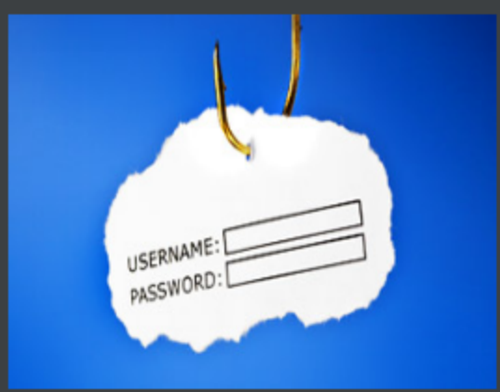
--Begin Transmission--

Spear Phishing

What is it?

Spearphishing is targeted phishing using spoof emails to persuade people within an organization to reveal sensitive information or credentials.

Unlike phishing, which involves mass-emailing, spearphishing is small-scale and well targeted. The attacker emails users in a single organization



The emails may appear to come from another staff member at the same organization, asking you to confirm a username and password.

Sometimes the emails seem to come from a trusted department that might plausibly need such details, such as IT or human resources.

Links in the emails will redirect to a bogus version of the company website or intranet for stealing credentials

Cybercrooks target select groups of people with something in common—they work at the same company, bank at the same financial institution, attend the same college, order merchandise from the same website, etc.

The emails are seemingly sent from organizations or individuals the potential victims would normally get emails from, making them even more deceptive.

How to avoid becoming a spear phishing victim

- Most companies, banks, agencies, etc., don't request personal information via e-mail.
- If in doubt, give them a call (but don't use the phone number contained in the e-mail—that's usually phony as well).
- Use a phishing filter.
- Never follow a link to a secure site from an email; always enter the URL manually.

--End Transmission--

Information Security: It's a Shared Responsibility

REFERENCES

http://blog.avast.com/tag/spearphising/

http://www.sophos.com/en-us/threat-center/threat-analyses/threatsaurus/a-to-z-of-threats/s/spearphishing.aspx

--End Transmission--

Document Code: 2014ICT_15SECA038