Phishing Attack Prevention: How to Identify & Avoid Phishing Scams

IT Department

Northern Lights College

2016

What is Phishing ?

- Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, Instant Messaging or other communication channels.

Overview

- No matter how secure the college's IT security platform is, the college is only as secure as its user base. Unfortunately, compromised credentials represent the vast majority of hacks (over 90%) and phishing and spear phishing attacks are responsible for the majority of those breaches.
- So, with all the investment capital devoted to securing IT infrastructure, how can companies prevent employees from opening phishing emails? The best answer is continuous, hands-on employee education and that is why you are reading this slide.

Phishing Techniques

There are various phishing techniques used by attackers:

- Embedding a link in an email that redirects you to an unsecure website that requests sensitive information
- Installing a Trojan via a malicious email attachment or ad which will allow the intruder to exploit loopholes and obtain sensitive information

Phishing Techniques cont’d

- Spoofing the sender address in an email to appear as a reputable source and request sensitive information
- Attempting to obtain company information over the phone by impersonating a known company vendor or IT department

Phishing “red flags” and countermeasures

- Any un-solicited communication regarding any account you have.
- Any un-solicited communication regarding any account you *don't* have. Un-solicited, or unexpected e-mail attachments.
- Requests for you to send your username and/or password, or other personal details.
- Proliferate spelling, grammar, or factual errors.
- An overwhelming emphasis on urgency
- Anything "too good to be true
- FROM addresses that don't match the REPLY address

Countermeasures

- **Stop, breathe, and think.** No matter what they tell you, don't let yourself get into any rush. If someone is initiating a contact with you, taking time out of your day, they can stand to wait a few minutes (or even hours) while you sort things out for yourself, and decide what you're going to do.
- **Do not offer any information.** This is what phishers want. Even if you're not giving them the specific information they're asking for, you may still be giving them something else they can use against you later.
- **Do not open any e-mail attachments.** Just. Don't. Do. It.
- **Do not follow any hyperlinks or URLs.** Again, just don't.

Do not reply.

Thanks for reading