THE FULCRUM GROUP

Concentration On Little Things Shows

THE SAFETY EDITION

What is Phishing and how does it affect me and our company?

Webster's defines it as:

phish·ing

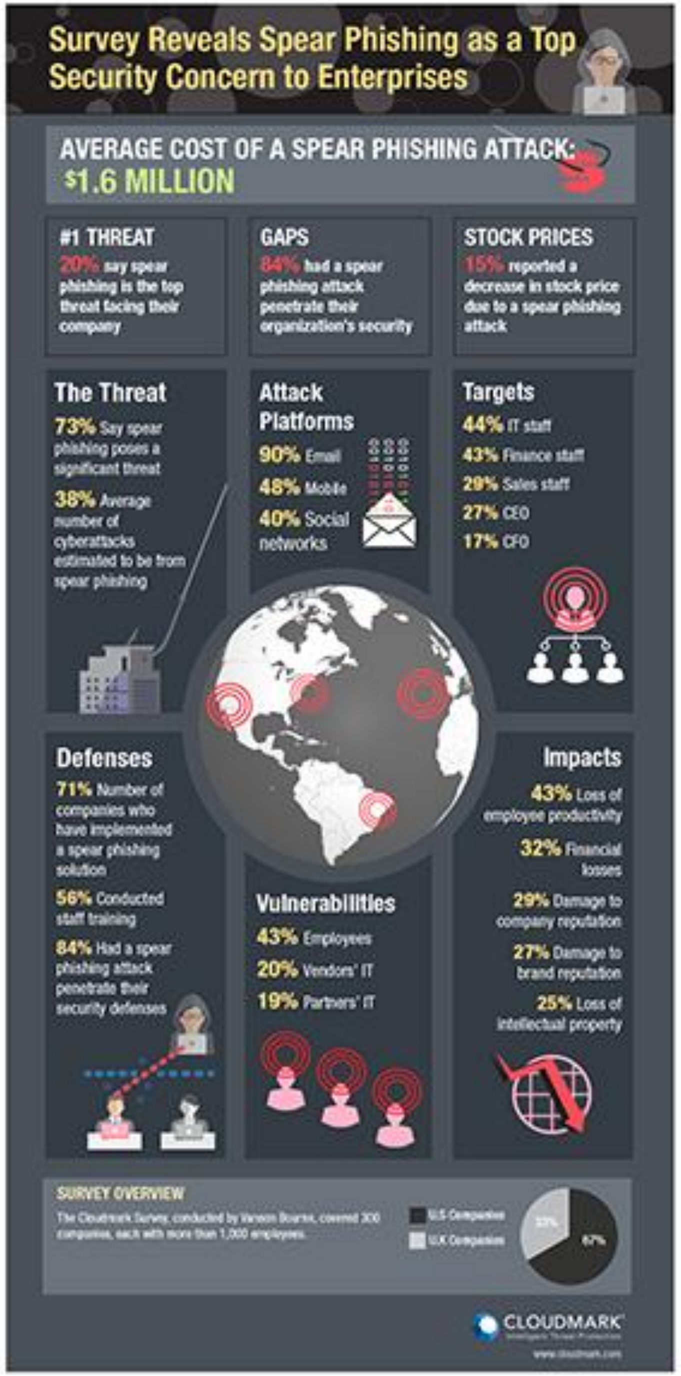
'fiSHiNG/

noun: **phishing**

- the activity of defrauding an online account holder of financial or personal information by posing as a legitimate company.
- "phishing exercises in which criminals create replicas of commercial Web sites or official looking emails"

It’s Big Business to Get Your Information

The main purpose of phishing is to gather personal and/or financial data about an individual or organization for the sole purpose of reselling for financial gain.



Survey Reveals Spear Phishing as a Top Security Concern to Enterprises

AVERAGE COST OF A SPEAR PHISHING ATTACK: $1.6 MILLION

#1 THREAT
20% say spear phishing is the top threat facing their company

GAPS
84% had a spear phishing attack penetrate their organization's security

STOCK PRICES
15% reported a decrease in stock price due to a spear phishing attack

The Threat
73% Say spear phishing poses a significant threat
38% Average number of cyberattacks estimated to be from spear phishing

Attack Platforms
90% Email
48% Mobile
40% Social networks

Targets
44% IT staff
43% Finance staff
29% Sales staff
27% CEO
17% CFO

Defenses
71% Number of companies who have implemented a spear phishing solution
56% Conducted staff training
84% Had a spear phishing attack penetrate their security defenses

Vulnerabilities
43% Employees
20% Vendors' IT
19% Partners' IT

Impacts
43% Loss of employee productivity
32% Financial losses
29% Damage to company reputation
27% Damage to brand reputation
25% Loss of intellectual property

SURVEY OVERVIEW
The Cloudmark Survey, conducted by Vanson Bourne, covered 300 companies, each with more than 1,000 employees.

Phishing affects everyone

In 2015, McAfee sent a 10 question quiz on various emails to 19,000 people spanning 140 countries to see if they could tell which ones were legitimate requests and which were deceptive.

- Only 3% got all 10 correct
- Only 78% of IT Professionals could identify all 10 correctly
- 80% incorrectly identified at least phishing email attempt
- The average score was 65.40%

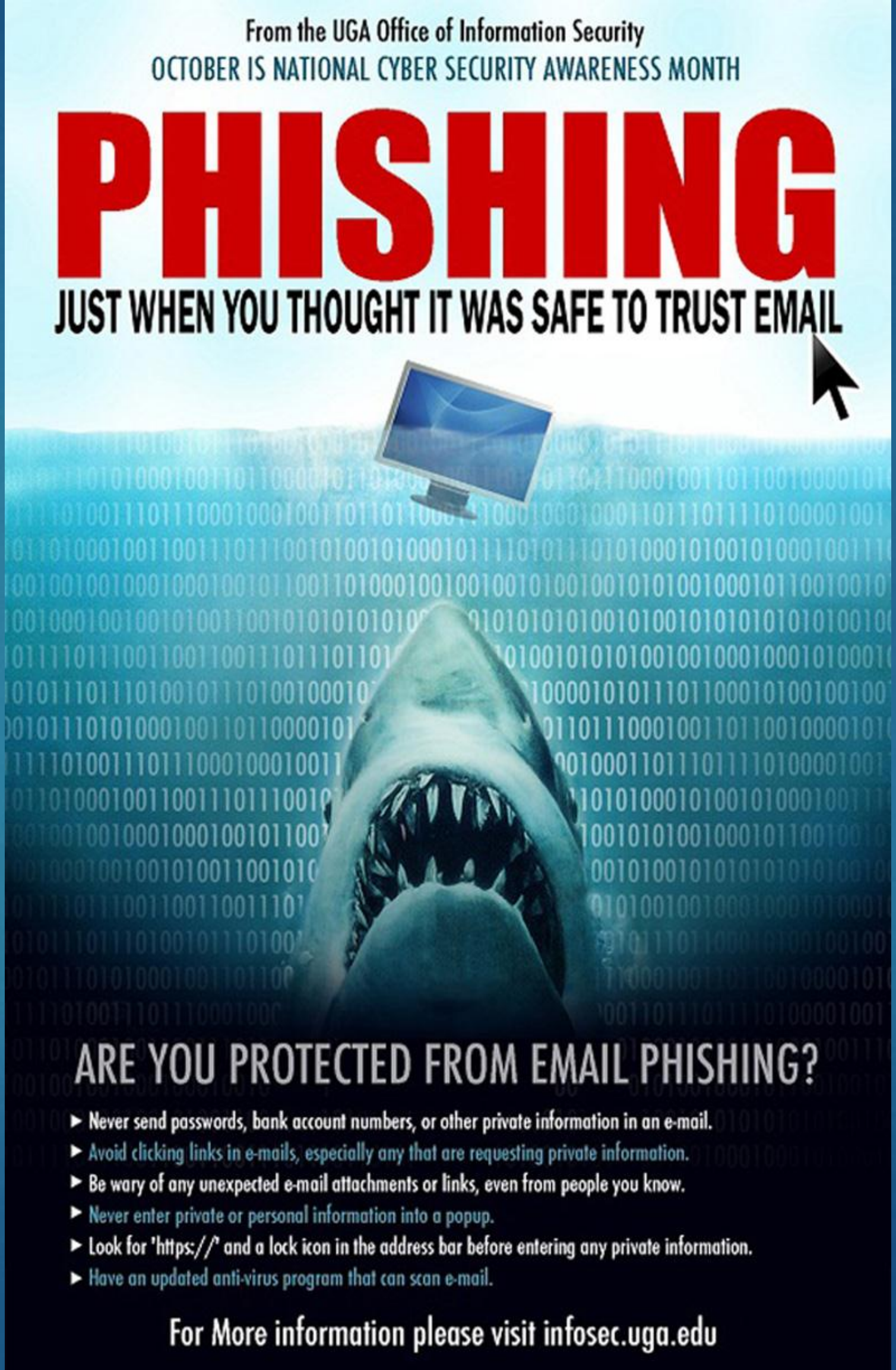
What Can We Do To Protect Ourselves?

- Hover over the web link to make sure that the URL and the link match.
- Never offer up personal/financial data on a website that is not secured (look for the padlock in the Address Bar).
- Don't get pressured into divulging information.
- Watch out for generic looking requests for information.
- When in doubt, don't click on that link, just open a web browser and type in the URL yourself.
- Do not open attachments unless you are 100% confident of the sender's reputaion.

How Can We Browse Safely on the Internet?

- Check and re-check web addresses, mouse over links to make sure the URLs match.
- Think before you click, don't just click through forms, be deliberate.
- Be wary of shortened links, as it hides their true destination.
- Stay alert, be suspicious of offers of free content or those too-good-to-be-true.
- Make sure Antivirus is up to date

- If you see any suspicious email or webpages, alert your manager and share your findings with coworkers.
- If you have become a victim of a phishing attack you need to immediately get in touch with the organization linked to the information leaked (Bank, Credit Card Company, Social Security, etc.)
- If your computer starts to behave erratically, it is best to get it off the network as soon as possible to avoid any chance that a virus infection could spread.
- Finally, be just as vigilant with these concepts on your mobile device.



From the UGA Office of Information Security

OCTOBER IS NATIONAL CYBER SECURITY AWARENESS MONTH

PHISHING

JUST WHEN YOU THOUGHT IT WAS SAFE TO TRUST EMAIL

ARE YOU PROTECTED FROM EMAIL PHISHING?

- Never send passwords, bank account numbers, or other private information in an e-mail.
- Avoid clicking links in e-mails, especially any that are requesting private information.
- Be wary of any unexpected e-mail attachments or links, even from people you know.
- Never enter private or personal information into a popup.
- Look for 'https://' and a lock icon in the address bar before entering any private information.
- Have an updated anti-virus program that can scan e-mail.

For More information please visit infosec.uga.edu