UNIVERSITY *of* WASHINGTON

Office of the Chief Information Security Officer

SPEAR PHISHING RISK ADVISORY

PHISHING VS. SPEAR PHISHING

Phishing is a form of email fraud aimed at enticing potential victims to provide login credentials and other information that can be exploited for either financial gain or access to valuable data and resources. Spear phishing targets particular individuals or groups, such as members of the University community, in order to trick them into providing credentials that can be used to access (and in some cases steal) specific types of information, such as intellectual property and research data, as well as resources in the University's libraries.

PREVALENCE AT UNIVERSITIES

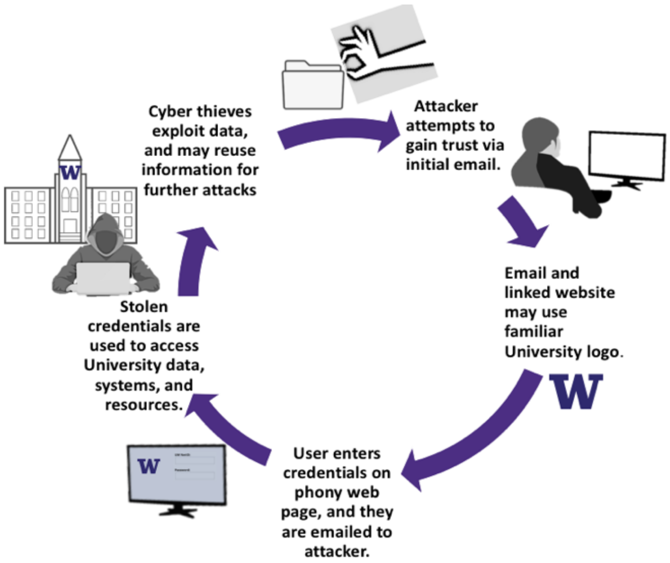
These types of attacks are leveraged against universities with some regularity. Recently, the U.S. Justice Department charged a group of cyber thieves with maliciously hacking hundreds of companies and academic institutions in order to steal more than $3.4 billion in trade secrets. A number of American universities—144 of them—were named in the case, and it is estimated that 31 terabytes of academic data and intellectual property were stolen from those institutions.[1]

Spear phishers often use information found on the Internet and on social media accounts to prepare email messages that are tailored to appeal to faculty, researchers, and others in academia. A typical message may reference specific works published by the targeted individual in order to look like a legitimate inquiry. Once a sense of trust is established, the phisher might dupe the victim into giving up data in a number of ways.

STAGES OF ATTACK

1. An initial email, or series of emails, is sent in which the phisher attempts to gain your trust;
2. The email and any web page it links to may be crafted to look like an official university communication, using a familiar logo and style;
3. When credentials are entered into the phony page, they are emailed to the cyber thieves;
4. Stolen credentials are then used to access the same information systems and resources that you log in to, such as your email, student and research data, and library accounts;
5. Cyber thieves can then exploit the data and resources in a number of ways for example, for financial gain or to steal valuable research or intellectual property.

[1] Mak, Aaron, "Justice Department Indicts Iranian Hackers for Allegedly Stealing Research From Hundreds of Universities," March 23, 2018, https://slate.com/technology/2018/03/iranian-hackers-department-of-justice-steal-university-research.html


Attacker attempts to gain trust via initial email.
Email and linked website may use familiar University logo.
W
User enters credentials on phony web page, and they are emailed to attacker.
W
Stolen credentials are used to access University data, systems, and resources.
Cyber thieves exploit data, and may reuse information for further attacks
W

BEST PRACTICES

1. As a rule, don't click on links in email.
   - Keep in mind that even familiar senders and links may be spoofed.
   - If it is absolutely necessary to click, hover over the link with your mouse to ensure the url revealed matches or corresponds to the link that appears in the message.
   - If you must access the linked information, determine what website you're being directed to, open a browser and use the search box to find the site and the information or resources described.
2. Don't download or open unfamiliar or unexpected attachments.
3. Don't enter password credentials in login pages linked from email.
4. Regard emails that solicit information of any kind with suspicion.
5. Be wary of emails that create a false sense of urgency, such as those that admonish you to verify or update information or threaten to delete your account.
6. Be aware that web pages that are linked from email may be crafted to look just like an authentic UW web login page.

LEARN MORE: https://ciso.uw.edu/education/#phishing

UW Office of the CISO, April 2018