Email Phishing Attack
(CSB19-02)

SUMMARY

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information. The email makes an offer that sounds too good to be true. It might say you've won the lottery, or some other over-the-top item.

SIGNS OF PHISHING

Unofficial "From" address.

Urgent action required. Hackers often include urgent "calls to action" to try to get your to react immediately. Be wary of emails containing phrases like "your account will be closed," "your account has been compromised," or "urgent action required."

Generic greeting. Hackers often send thousands of phishing emails at one time. Be skeptical of an email sent with a generic greeting.

Link to a fake website. Hackers often include a link to a fake website that looks like the sign-in page of a legitimate website

Legitimate links mixed with fake links. Hackers include authentic links mixed in with links to a fake phishing website in order to make the spoof site appear more realistic.

HOW IT WORKS

An attacker sending out thousands of fraudulent messages

The recipient is advised to click on the link or open the attachment

Once click, it will be redirected to a fake website and will ask for credentials

Credentials are stolen

MITIGATION

Two-factor authentication prevents the use of compromised credentials.

Enforce strict password management policies. Employees should be required to frequently change their passwords and to not be allowed to reuse password for multiple applications.

Do not click on a link inside of an email from unknown sender.

SECURITY RISKS

- Credentials can be stolen such as username and passwords; and
- Hackers can attack your contact list by pretending to be you.

REFERENCES

- CSB18-03 (Revised March 14, 2018) Phishing
- https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html
- https://www.malwarebytes.com/phishing/
- https://safety.yahoo.com/Security/PHISHING-SITE.html