United States Secret Service [INFO]

January 25, 2019

[INFO] Information Only Alert – GIOC Reference #19-002-I
TLP Green

Phishing Campaigns on the Rise

The Secret Service's Global Investigative Operations Center (GIOC) is observing a noticeable increase in successful large-scale phishing attacks targeting unsuspecting victims across industry. Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. The fraudsters will typically send victims an email that appears to originate from a credible source containing a link which appears to be from their financial institution (FI) or employer, and requests a login or password reset. This link directs the victim to a spoofed website controlled by the fraudsters.

The recent successful phishing campaigns leverage all spoofed employer and financial institution websites to trick the victim into believing they are transacting on a legitimate website.

Tax season is rife with this type of fraud. The Secret Service annually investigates frauds targeting victims expecting tax returns and human resources employees in an attempt to obtain W-2 and other tax related documents.

Quick tips on how to avoid these compromises:

- Never click on links embedded in emails or open any attachments from an unknown or suspected fraudulent email account.
- Always independently verify any requested information originates from a legitimate source.
- Visit websites by inputting the domain name yourself. If needed, then update/change your information.
- If you are contacted over the phone, hang up, look up the phone number for the institution, and call back. Do not give your information over the phone.

Any questions relating to this alert can be directed to the GIOC at gioc@usss.dhs.gov or 202-406-6009.

[INFO] - Indicates informational or educational content.