

[Heads-up] Cyber Criminals Refine Their Social Engineering Tactics

Attackers are improving their strategies by accounting for new developments in technology, Help Net Security reports. Researchers at FireEye analyzed 1.3 billion phishing emails and identified three major trends in Q1 2019.

First, attackers are increasingly using **impersonation** in their phishing attacks. Impersonation attacks in 2019 have increased 17% over Q4 2018, primarily imitating well-known brands. Attempts to spoof Microsoft accounted for nearly a third of these attacks, with OneDrive, PayPal, Apple, and Amazon. More targeted CEO impersonation attacks are also on the rise, and FireEye's Ken Bagnall expressed concern that organizations don't understand the level of sophistication that these attacks employ.

"We're seeing new variants of impersonation attacks that target new contacts and departments within organizations," said Bagnall. "The danger is these new targets may not be prepared or have the necessary knowledge to identify an attack. Unfortunately, once the fraudulent activity is discovered, the targeted organization thinks they've paid a legitimate invoice, when the transaction was actually made to an attacker's account."

A second trend is the **increased use of HTTPS** for phishing sites, which jumped by 26% in Q1 2019. These certificates are free and easy to obtain for any website. Since most browsers automatically flag non-encrypted connections as insecure, an SSL certificate is becoming an essential component for any site that wants its users to feel safe. This trend, coupled with the widespread misconception that an HTTPS connection alone is a sign of legitimacy, means that the use of HTTPS will continue to become a standard feature in phishing campaigns.

Finally, attackers are turning to **cloud-based attacks** using trusted services such as **Dropbox, Google Drive, and OneDrive**. By hosting malicious files on these services, attackers can send links that don't look suspicious to users and that can get through email filters.

Most people assume that they'll be able to spot a scam when they see one, so it's not something they factor into their thinking. Employees who are expecting to be targeted by social engineering attacks will be far more vigilant as they carry out routine activities.

Knowbe4, July 2019