Issued 3/14/17

Phishing: Would You Fall For One Of These Scam Emails?

Phishing scams aim to trick staff into handing over data -- normally usernames and passwords -- by posing as legitimate email. It's a technique used by the lowliest criminals as part of ransomware campaigns, right up to state-backed hackers because it continues to be such an effective method

In a review of 100 simulated attack campaigns for 48 of its clients, accounting for almost a million individual users, security company MWR Infosecurity found that sending a bogus friend request was the best way to get someone to click on a link -- even when the email was being sent to a work email address.

A spoof email claiming to be from the HR department referring to the appraisal system was also very effective: nearly one in five clicked the link, and three-quarters provided more credentials, with a similar percentage going on to download a file.

Some might argue that gaining access to a staff email account is of limited use, but the security company argues that this is a handy for an assault. A hacker could dump entire mailboxes, access file shares, run programs on the compromised user's device, and access multiple systems, warned MWR InfoSecurity.