Tech Essentials for Insurance Professionals

An RPost
E-Brief Series

Online Ads Provide Hacker Entry Point

In a recent *Tech Essentials* article ("Changing Trends in Cyber Security"), we highlighted how hackers are becoming more innovative in their ability to use generally available social media (i.e. LinkedIn recruiter tools) and other business applications to target email recipients with imposter email and lure them into wiring money to hackers.

This upfront investment (in social media marketing tools, for example) permits hackers to tailor their message such that it appears authentic, increasing their likelihood of extracting money from their intended victims.

Another tactic that hackers are beginning to exploit involves use of popular online advertising platforms (such as Google, Facebook, etc.) to obtain the Internet Protocol (IP) address of the person viewing a hacker-placed advertisement. This common technique, one that legitimate advertisers rely on to gain demographic information associated with their audience, provides hackers with a means to identify each ad viewer's specific Internet Service Provider (ISP).

Armed with ISP information, the hacker is then able to set up "re-marketing" ads that target each ad viewer with a banner ad that contains a falsified message and images pertaining to each viewer's specific ISP -- Time Warner Cable, or Verizon, for example. These re-marketing ads might, for example, claim to be a message from the specific ISP's tech support team, telling the viewer that their computer is infected. A telephone number is displayed, instructing the viewer to call to fix the computer. This phone number goes to a hacker-directed call center, where an imposter poses as the ISP's tech support specialist. From there, the imposter support person might convince a victim to pay him/her a few hundred dollars to remove the virus, as a premium support service. Further, the imposter might instruct the victim to provide remote access to their computer. With remote access, the imposter support staff is able to secretly access personal files – all while opening standard system folders in the foreground to misdirect the victim.

Sound elaborate? This scam works, and its success is leading more hackers to jump in. It has been reported that one hacker made $17 million over the course of several months by persuading people to sign up for bogus tech support services and give credit card details that provided the scammers with a one-off payment of around $200 each (along with the opportunity to rack up fraudulent charges in the future). At the moment, the main target profile is consumers using Gmail, Yahoo mail, Microsoft Outlook.com/Hotmail, Verizon email, Time Warner Cable email, and AT&T email, accessed from Verizon, AT&T and Time Warner Cable ISP access.

People are literally paying to be scammed.