FEBRUARY 2015

Security Awareness Newsletter

Targeted and Personal

Executives are often the targets of highly personal attacks. Here's a real world example described in Chris Hadnagy's book, Social Engineering: The Art of Human Hacking.

Chris was hired to try to access a company's proprietary processes and sensitive information. The company's CEO told Chris that "hacking him would be next to impossible" because he "guarded his secrets with his life."

Through Facebook, Chris learned that the CEO had a family member who survived cancer and that the CEO was involved in cancer fundraising. He also learned the names of the CEO's favorite restaurant and sports team.

Posing as a fundraiser from a cancer charity, Chris called the CEO and got him to agree to look at a PDF file describing a fund raising event where the CEO could buy tickets for a drawing for a season pass to the CEO's favorite sports team and gift certificates to his favorite restaurant.

When the CEO opened the PDF, malicious code was installed that allowed Chris to access the CEO's machine.

The CEO said it was unfair for Chris to use personal information and lying to gain unauthorized access. Chris pointed out that a malicious hacker wouldn't think twice about using such practices.

The bottom line: Attackers will use any information, including information of a personal nature

Senior Executives Blamed

In October 2013, Opinion Matters for ThreatTrack conducted a blind survey of 200 security professionals. The survey found that 66 percent have faced a security incident which could be tracked back to a senior executive.

Respondents cited policy violations and careless behavior as the most common causes. The top reasons given were: installation of a malicious mobile application (33 percent); allowing a family member to use the company-owned device (45 percent); phishing (56 percent); or accessing pornographic websites (40 percent).

Steve Ragan, writing for Network World News, said, "Criminals target people first and platforms second, and in IT it's an unfortunate reality that most executives are exempt from policy enforcement and security restrictions. […] When people become low-hanging fruit easy for the picking due to blatant disregard for, or an absence of, security policy -- criminals have a readymade attack surface to exploit." [Network World News]

Common Phishes

- Subpoena phish. This attack targets company executives. The phish email arrives late on a Friday afternoon and claims that the executive has been subpoenaed, and must give evidence at 10 am on Monday morning — or… if that time isn't suitable, just "click here" to change your appointment time. And, now that people are posting so much information about their lives on social networking sites, it's easy for an attacker to construct a plausible scenario.

- Better Business Bureau Complaint phish. In this phishing attack, the target receives an official-looking email that appears to be a complaint from the Better Business Bureau. The email has a link for the target to contest or respond to the claim. If the link is clicked, malware is installed.

Image via Shutterstock.com

email: InfoSec@yourcompany.com