Hacking the Human: Social Engineering

Most businesses rely on a network to collect, store, transfer and dispose of sensitive data. From Social Security Numbers, W-2 forms, payment cards, and intellectual property, securing that data continues to be a challenge as hackers can easily monetize this data on the black market.

According to the FBI, from October 2013 to August 2015, more than **8,000 social engineering victims** from across the United States **were defrauded of almost $800 million**.

The average loss amounted to **$130,000.**

Many businesses install technological defenses to prevent data theft. Criminal perpetrators, however, remain one step ahead of even the best cybersecurity efforts. They have altered their strategies by perpetrating human-based fraud. One emerging tactic involves what is currently called social engineering fraud. Social engineering fraud occurs in a multi-stage process. Criminals gather information, form relationships with key people, and execute their plan, often through email.

News reports highlight massive criminal activity of stolen credentials that include email usernames and passwords of U.S. banking, manufacturing and retail companies.*

Criminals have been highly successful in convincing people to hand over their most valuable data assets. In fact, according to the FBI, from October 2013 to August 2015, more than 8,000 social engineering victims from across the United States were defrauded of almost $800 million. The average loss amounted to $130,000.

There are several methods of social engineering fraud that are seen frequently, including the following:

- **Bogus Invoice:** A business that has a long standing relationship with a supplier is asked to wire funds to pay an invoice to an alternate, fraudulent account via email. The email request appears very similar to a legitimate account and would take very close scrutiny to determine if it was fraudulent.
- **Business Executive Fraud / Email Phishing:** Email accounts of high-level business executives (CEO, CFO, etc.) may be mimicked or hacked. A request for a wire transfer or other sensitive information from the compromised email account is made to someone responsible for processing transfers. The demand is often made in an urgent or time sensitive manner.
- **Interactive Voice Response/Phone phishing (aka vishing):** Using automation to replicate a legitimate sounding message that appears to come from a bank or other financial institution and directs the recipient to respond in order to “verify” confidential information.
- **Dumpster diving & forensic recovery:** Sensitive information is collected from discarded materials such as old computer equipment, printers, paper files, etc.
- **Baiting:** Malware-infected removable media, such as USB drives, are left at a location where an employee may find it. When they attach the USB to their own computer, criminals can ex-filtrate valuable data.
- **Tailgating:** Criminals gain unauthorized access to company premises by following closely behind an employee entering a facility, or by presenting themselves as someone who has official business with the company.
- **Diversion:** Misdirecting a courier or transport company and arranging for a package or delivery to be taken to another location.

HUB

HOW TO AVOID BEING DEFRAUDED

Given the rising incidence of social engineering fraud, all companies should implement basic risk avoidance measures:

- **Educate your employees** so that they can learn to be vigilant and recognize fraudulent behavior.
- **Establish procedures** requiring any verbal or emailed request for funds or information transfer to be confirmed in person or via phone by the individual supposedly making the request.
- **Consider two-factor authorization** for high level IT and financial security functions and dual signatures on wire transfers greater than a certain threshold.
- **Avoid free web-based email** and establish a private company domain and use it to create valid email accounts in lieu of free, web-based accounts.
- **Be careful of what is posted to social media** and company websites, especially job duties/ descriptions, hierarchal information, and out of office details.
- **Do not open spam or unsolicited email** from unknown parties, and do not click on links in the email. **Do not use the "Reply" option** to respond to any financial emails. Instead, use the "Forward" option and use the correct email address or select it from the email address book to ensure the intended recipient's correct email address is used.
- **Beware of sudden changes** in business practices. For example, if a current business contact suddenly asks to be contacted via their personal email address when all previous official correspondence has been on a company email, the request could be fraudulent.

Contact a HUB Cyber Risk advisor to help you with education, training and mitigation of social engineering fraud. Let's get started in building a plan that secures your most valuable information and data.

HUB

* Source: http://www.businessinsurance.com/article/20160504/NEWS06/160509937?X-IgnoreUserAgent=1