March 2017

Protection from Social Engineers

Social engineering, one of the most common tools in a hacker's arsenal, plays a role in many security breaches, which feature prominently in global media reports.

Larry Zelvin
Director of the Citi Cyber Security Fusion Center (CSFC)

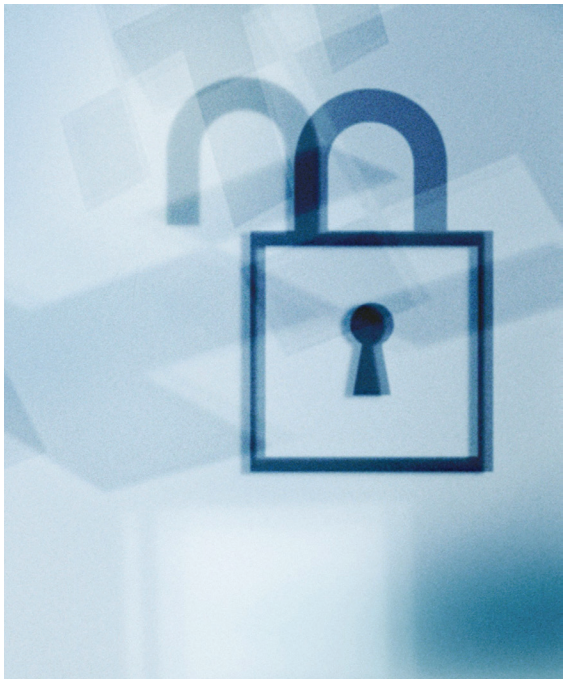
In the most general sense, social engineers attempt to influence or manipulate human behavior, often by constructing an environment in which the victim is likely to comply with the hacker's goals, such as by clicking on a link, visiting a website, submitting a password or providing other information that the hacker is seeking.

Successful social engineers gather information, often public or widely available, and customize an email, phone call or other communication to a victim, so that it appears to be valid.

Phishing

Phishing is a tactic frequently used by social engineers. Phishing is the act of attempting to acquire information or induce a victim to click on a malicious link by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social websites, online payment processors or IT administrators are commonly used by hackers to deceive potential victims. More targeted phishing emails may purport to be sent from the victim's alma mater, a charity he or she is known to work with, or an institution of which the victim is a known client.

Phishing emails may contain links to websites that are infected with malware and often direct users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Success lies in convincing the recipient that the source of the communication is the spoofed company itself (by virtue of research, the attacker knows that the recipient trusts the entity in question), so that the recipient will provide the requested information.



Examples

Phishing emails often take advantage of events in the news, or topics trending on social media. During the 2010 earthquake in Haiti, for example, social engineers sent phishing emails telling recipients that a family member was arrested while volunteering with the Red Cross in Haiti. Emails such as this aim to appeal to a victim's sense of urgency and capitalize on real-time events to do so. While individuals who receive the email are more likely to click on a link or believe this information, this tactic would likely be unsuccessful at a different point in time where the scenario in question (here, that a family member was volunteering for a specific incident) lacked the necessary context.

Similarly, in the wake of Hurricane Sandy in 2012, emails stating the following were sent: "Thank you for your donation to Hurricane Sandy relief. We appreciate your donation of 435 dollars. Credit card on file has been charged. If you did not authorize donation please go to (website URL) to unauthorize the charge. Thank you again for your donation, Red Cross." Here, recipients may be inclined to click on the link to investigate. Again, absent the pretext of the event, it is unlikely that a potential victim who received the email would click on the link.

Digital Footprint

If you are a client of the Commercial Bank, it is likely that you have an online presence of some sort. Perhaps your title and a description of your background and experience are provided on your company's website. You may have contributed to philanthropic organizations, your alma mater or a cause you care about, and these organizations may have publically acknowledged your contribution. Moreover, there is a good chance you have social media presence — whether it's on LinkedIn, Facebook or Twitter — and as a result, information about your life is likely accessible to some degree.

To the extent possible, it is often recommended that you configure all possible security settings on social media to minimize information that is indiscriminately accessible to the public. It is not difficult for cybercriminals to identify a potential trigger and craft an email tailored specifically for a target such as yourself. According to the National Counter Intelligence and Security Center, 15% of social media users publically share their birthday, 17% post the name of the high school they attended, and 29% of users do not use strong passwords to protect their accounts. For example, the hacker who claimed responsibility for the breach of a high-ranking member of the federal government's email account, reportedly gained access by socially engineering his way to his data. This would not have been possible if the hacker did not have access to certain personal information.

Considerations

Personal information can be used against you in a growing number of ways. In order to protect yourself, it is recommended that Commercial Bank clients consider the following security measures:

- To the extent it is possible, limit the amount of personal information shared on social media sites by you and your immediate family members.
- Secure social media profiles with strict privacy settings and don't accept connection requests from strangers.
- Verify the identities of all contacts (do not rely on the "from" display).

For example, remember: Citi will NEVER do the following:

- Send urgent or time-sensitive emails, or ones that ask you to provide, update or confirm sensitive data like your Online User ID or Password, PIN, SSN, ATM/Debit Card or account number, credit card number or expiration date, or mother's maiden name.
- Send you an email that tells you to provide personal information because it's for your own security.
- Send you an email with input fields that ask you for sensitive information.