SOCIAL ENGINEERING

Techniques, Tactics and Countermeasures
November 2015
Social Engineering: Human Exploits

Social engineering is a broad term for a wide range of techniques used by criminal attackers that exploit the human element. While cyber attacks combine a range of different tactics, it is clear that there is one very common risk denominator – us humans.

Social engineering tactics and techniques are components of many, if not most cyber attacks and the primary channel through which attacks are initiated. This is a trend that is likely to continue as businesses ramp up their IT security infrastructure, criminals will just turn more focus on the weak human infrastructure.

According to the Verizon 2015 DBIR report, humans or users account for 90% of security incidents. Symantec and Cisco recently released reports that echo Verizon’s “People” findings


<table>
<thead>
<tr>
<th>Category</th>
<th>Incidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miscellaneous Errors</td>
<td>29.4%</td>
</tr>
<tr>
<td>Crimeware</td>
<td>25.1%</td>
</tr>
<tr>
<td>Insider Misuse</td>
<td>20.6%</td>
</tr>
<tr>
<td>Physical Theft or Loss</td>
<td>15.3%</td>
</tr>
</tbody>
</table>

While the threats against us may “seem” innumerable, infinitely varied, and ever-changing, the reality is they aren’t. The common denominator across the top four patterns of security incidents – accounting for nearly 90% of incidents – is people. Whether it’s goofing up, getting infected, behaving badly or losing stuff.”

- Verizon 2015 DBIR

Verizon 2015 DBIR Report – Internal Actors within Insider Misuse Category

<table>
<thead>
<tr>
<th>Actor</th>
<th>Incidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>End User</td>
<td>37.6%</td>
</tr>
<tr>
<td>Cashier</td>
<td>16.8%</td>
</tr>
<tr>
<td>Finance</td>
<td>11.2%</td>
</tr>
<tr>
<td>Executive</td>
<td>10.4%</td>
</tr>
<tr>
<td>Other</td>
<td>8%</td>
</tr>
<tr>
<td>Manager</td>
<td>6.4%</td>
</tr>
<tr>
<td>Developer</td>
<td>5.6%</td>
</tr>
<tr>
<td>Call Center</td>
<td>4%</td>
</tr>
<tr>
<td>Systems Administrator</td>
<td>1.6%</td>
</tr>
<tr>
<td>Help Desk</td>
<td>0.08%</td>
</tr>
</tbody>
</table>

This year, Verizon reported seeing more incidents involving end users than ever before, which is alarming, considering the vast majority of regular end users make up the population of any given enterprise.
Almost no company, whether large or small, is immune to spear-phishing. Five out of six large (2,500 + employees) companies were targeted with spear-phishing attacks during 2014 – a 40 percent increase over the previous year. Small and medium-sized businesses also saw an uptick, with attacks increasing 26 percent and 30 percent, respectively.”

– Symantec 2015 Internet Security Threat Report (ISTR)

Humans are the roots cause of attacks, the primary targets of attacks and now complicit enablers of attacks!

Adversaries are committed to continually refining or developing new techniques that can evade detection and hide malicious activity. Meanwhile, the defenders –namely, security teams –must constantly improve their approach to protecting the organization and users from these increasingly sophisticated campaigns. Caught in the middle are the users. But now, it appears they not only are the targets, but also complicit enablers of attacks.”

– CISO 2015 Annual Security Report
Social Engineering

Social engineering is just a con job, the tactics are the methods and the techniques are the style of exploit(s) the criminal chooses to use.

Social Engineering Tactics

- Virus writers try to persuade people to run malware by clicking on links in emails
- Phishers try to convince people to divulge sensitive or confidential information
- Scareware vendors try to frighten people into giving them access to networks
- Ransonware vendors threaten people into giving them money by holding networks or data for ransom

Social Engineering Techniques

**Baiting** is leaving malware-infected devices in places it is sure to be found. The finder then picks up the device and loads it onto his or her computer, unintentionally installing the malware.

**Phishing** is sending a fraudulent email disguised as a legitimate email meant to trick the recipient into sharing personal or installing malware on his or her computer or device.

**Smishing** is phishing that starts with texting.

**Spear-Phishing** is like phishing, but focused or targeted to a specific individual, a group of individuals with commonalities (affinity/focus/alumni/professional associations) or organizations.

**Vishing** is voice to voice phishing or phishing phone calls.

**Pre-texting** is when one party lies to another to gain access to privileged data. A pre-texting scam could involve an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.

**Quid Pro Quo** is when an attacker requests personal information from a party in exchange for something desirable. For example, an attacker could request login credentials in exchange for a free gift or a coupon.

**Tailgating** is when an unauthorized party follows an authorized party into an otherwise secure location, usually to steal valuable property or confidential information.

**Farcing** is a scam involving a phony social profile, which a scammer creates and then uses to connect with strangers in an attempt to obtain personal information.

**Spam** is good old fashioned unsolicited junk email.
Counteracting Social Engineering Attacks

The security of a business largely depends on the level of its users’ data privacy and security awareness. Many studies have shown that providing employees with proper Data Privacy & Security training significantly reduces social engineering attacks.

A recent Ponemon Study sponsored by Wombat Security Technologies, concluded that the average 10,000-employee company spends $3.7 million a year dealing with phishing attacks. However, businesses can substantially reduce their phishing-related costs with employee education. Businesses that roll out training programs see improvements of between 26 and 99 percent in their phishing email click rates, with an average improvement of 64 percent, according to Ponemon. Other key findings include:

- The average total cost for an average company to contain malware is $1.9 million per year.
- Uncontained malware costs an average sized company as much as $105.9 million.
- The cost of business disruption due to phishing is $66.9 million.
- Employees waste an average of 4.16 hours annually due to phishing scams.
- The average annual cost to contain a credential compromise that originated from a successful phishing attack is $381,920.

A new study by Kaspersky Lab shows that in the last 12 months every fourth Internet user had at least one of their online accounts hacked. This led to unauthorized messages being sent out in the user’s name, and the loss or theft of personal data. The study was of users (a/k/a humans) and these users are employees. Therefore, every single personal account hack has the potential to grow into a full-scale cyber attack against a business.

The Carnegie Mellon study “Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions”, found that before specific training study participants on average fell for 47% of phishing attempts. After the training, this number was reduced to 28% - a 40% improvement.

Simulated or mock social engineering attacks can be a useful tool to quickly and effectively assess how susceptible employees are to phishing and spear phishing attacks. This allows security teams to know which users pose a risk and thus can take steps to provide additional training to remediate those risks. These simulated exercises and penetration testing are offered by most Information Security firms today.

The United States Computer Emergency Readiness Team (US-CERT) provides free information on their website including the latest information on cyber threats and vulnerabilities, how to avoid phishing attacks and what steps victims can take to protect themselves. For easy reference, excerpts from the US-CERT website are provided on the following page.

Sources:
http://info.wombatsecurity.com/cost-of-phishing
https://www.us-cert.gov/ncas/tips/ST04-014
Avoiding Social Engineering and Phishing Attacks

How do you avoid being a victim?

Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a website's security (see Protecting Your Privacy for more information).
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (see Understanding Firewalls, Understanding Anti-Virus Software, and Reducing Spam for more information).
- Take advantage of any anti-phishing features offered by your email client and web browser.

What do you do if you think you are a victim?

If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.

- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- Watch for other signs of identity theft (see Preventing and Responding to Identity Theft for more information).
- Consider reporting the attack to the police, and file a report with the Federal Trade Commission (http://www.ftc.gov/).