THE BIGGEST DANGER IS YOUR COMPLACENCY

“Success breeds complacency. Complacency breeds failure. Only the paranoid survive.”

- Andrew Grove, former CEO of Intel
IC3 statistics showing an increase in reports and reported losses since 2011.
SOCIAL ENGINEERING - HOW DOES IT WORK?

HACKER?
Social engineering is an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.

SOCIAL ENGINEERING IS THE #1 THREAT OF ALL SECURITY INCIDENTS ARE CAUSED BY YOU!
5 METHODS OF SOCIAL ENGINEERING

• **BAITING**: Baiting is when an attacker leaves a malware-infected physical device, such as a USB flash drive in a place 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**: Phishing is when a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source. The message is meant to trick the recipient into sharing personal or financial information or clicking on a link that installs malware.

• **SPEAR PHISHING**: Spear phishing is like phishing, but tailored for a specific individual or organization.

• **PRETEXTING**: Pretexting is when one party lies to another to gain access to privileged data. For example, a pretexting scam could involve an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.

• **SCAREWARE**: Scareware involves tricking the victim into thinking his computer is infected with malware or has inadvertently downloaded illegal content. The attacker then offers the victim a solution that will fix the bogus problem; in reality, the victim is simply tricked into downloading and installing the attacker's malware.
SOCIAL ENGINEERING CYCLE

1. Gather Information
2. Plan Attack
3. Acquire Tools
4. Attack
5. Use acquired knowledge
6. System Users

- Gather Information → System Users
- Plan Attack → System Users
- Acquire Tools → System Users
- Attack → System Users
- Use acquired knowledge → System Users
YOUR INFO USED AGAINST YOU
147 MILLION PEOPLE HACKED

Cybercriminals Use This Data To:

- Open credit cards and take out loans in your name.
- Steal your tax refund by filing a return with your name.
- Create highly targeted phishing scams to access your bank account, e-mail, computer and network.

<table>
<thead>
<tr>
<th>DATA ELEMENT STOLEN</th>
<th>IMPACTED U.S. CONSUMERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>147 million</td>
</tr>
<tr>
<td>Date of birth</td>
<td>147 million</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>146 million</td>
</tr>
<tr>
<td>Address</td>
<td>99 million</td>
</tr>
<tr>
<td>Gender</td>
<td>27 million</td>
</tr>
<tr>
<td>Phone number</td>
<td>20 million</td>
</tr>
<tr>
<td>Driver's license number</td>
<td>18 million</td>
</tr>
<tr>
<td>Email address</td>
<td>2 million</td>
</tr>
<tr>
<td>Credit card number</td>
<td>209,000</td>
</tr>
<tr>
<td>Tax ID</td>
<td>97,500</td>
</tr>
<tr>
<td>Driver's license state</td>
<td>27,000</td>
</tr>
</tbody>
</table>

Source: Securities and Exchange Commission filings from Equifax.
<table>
<thead>
<tr>
<th>Year</th>
<th>Company</th>
<th>Accounts Compromised</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>Marriott</td>
<td>500m</td>
</tr>
<tr>
<td>2017</td>
<td>Equifax</td>
<td>143m</td>
</tr>
<tr>
<td>2016</td>
<td>Adult Friend Finder</td>
<td>412.2m</td>
</tr>
<tr>
<td>2015</td>
<td>Anthem</td>
<td>78.8m</td>
</tr>
<tr>
<td>2014</td>
<td>eBay</td>
<td>145m</td>
</tr>
<tr>
<td></td>
<td>JP Morgan Chase</td>
<td>76m</td>
</tr>
<tr>
<td></td>
<td>Home Depot</td>
<td>56m</td>
</tr>
<tr>
<td>2013</td>
<td>Yahoo</td>
<td>3b</td>
</tr>
<tr>
<td></td>
<td>Target Stores</td>
<td>110m</td>
</tr>
<tr>
<td></td>
<td>Adobe</td>
<td>38m</td>
</tr>
</tbody>
</table>
• Separate your Home network from your Work Network
• Use Strong WIFI Encryption
• Regularly Update firmware on your router
• Use enterprise level endpoint protection and VPN software
25 Most Commonly Stolen Passwords

Protect yourself—and your company—by making sure you’re not using one of the top 25 most commonly stolen passwords of 2017, as determined by IT security firm SplashData.

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou
11. admin
12. welcome
13. monkey
14. login
15. abc123
16. starwars
17. 123456789
18. dragon
19. passw0rd
20. master
21. hello
22. freedom
23. whatever
24. qazwsx
25. trustno1
A STRONG PASSWORD

• Use a minimum password length of 12 to 14 characters if permitted.
• Include lowercase and uppercase alphabetic characters, numbers and symbols if permitted.
• Generate passwords that are not obvious (e.g., avoid using common passwords for user accounts and/or software systems).
• Avoid using personal information that the user or the account. Avoid using information that the user's colleagues and/or acquaintances might know to be associated with the user.
• Do not use passwords which consist wholly of any simple combination of the aforementioned weak components.

NEVER MIND ALL THAT-
USE LASTPASS & USE 2FA
NEVER REUSE PW
• Use a Dedicated “Work” Room W/ Lockable Door
• Do NOT allow anyone else to use your Work Computer
• Be sure Laptops are encrypted and that your screen is set to automatically log out
• Print as few Docs as possible, shred ASAP