Hacking Social Media

Your footprint is a hackers entrance

Dr. Chanel Suggs – Duchess of Cybersecurity ®
Agenda

• Defining Social Engineering
• Hackers vs You
• Social Media In-depth
• Social Media Threats
• Protection Techniques
• Hacking Techniques
• Attack Mode
• Women in IT/Cybersecurity
• Organizations
Defining Social Engineering

- Social engineering is techniques that are used by hackers to lure victims to reveal confidential information.

- This allows hackers to:
  - Infect systems with malware
  - Access infected sites
  - System being used for others means such as Botnets

- Social engineers depend on the fact that people are aware of certain valuable information and are careless in protecting it.
Why Hack?

• Most often reasons are to:
  • Steal Money
  • Promote political agendas
  • Cyber-espionage
  • Fame
  • Fun

• Most hackers make $350,000 or more per year
Hackers vs. You

- Hackers are always looking for flaws within computers, networks or mobile devices.
- Hackers typically have an advanced knowledge of program languages.
- It takes patience when it comes to hacking systems.
- People use generic passwords and share all online.
- Tools accessible to hackers makes it’s easy to crack these passwords.
- Your footprint online provides easy access for hackers.
Social Media Misconceptions

• Social media posting can be completely deleted.
• Using social media while on public Wi-Fi are protected networks.
• Profile information makes it easier to be connected with others and should be fully completed.
• No one has access to your information unless you allow it.
• Everything you place in your profile such as preferences, political opinions, comments doesn’t interest anyone that could harm you.
• Negative comments about employers or the government aren’t accessible to anyone without your approval.
Social Media Threats

- Social Engineering
- Phishing Attacks
- Fake Accounts
- Celebrity Spoofing
- Compromised Sites
- Fake Social Media Links
- Information Leakage
Social Media Precautions

• Social media posting can’t be completely deleted.
• Passwords need unique qualities, regular updating and a credible password manager.
• Using social media while on public Wi-Fi hotspots allows for it to be accessed by anyone utilizing that hub.
• Profile information creates a goldmine of info for hackers, the kind of data that helps them personalize phishing scams.
• Everything you place in your profile – personal preferences, political opinions, social commentary and more – is exposed even if you control the privacy settings.
• Any negative comments about an employer are accessible to that employer without any expectation of personal privacy.
Social Media Hacks: mSpy

• A mobile and computer monitoring software for iOS, Android, Windows, and macOS. It monitors and logs user activity on the device.
  • Extremely reliable services
  • GPS location of target available
  • Keylogger facility is a great advantage
  • Get logs of all incoming and outgoing calls
  • Have access to internet browsing history
  • Monitoring messengers on Facebook Viber, WhatsApp, Line, etc.
  • Read all texts and view shared photos and videos
  • You can view and manage any function a phone does, including Facebook messenger.
  • Spy on chats
  • Monitor and manage installed apps
  • Monitor calls as well as people listed within the phone book
Social Media Hacks: mSpy

Simplest way to hack Instagram password.

• Open your phone open the Instagram app
• Go to menu options, click ‘Add account’
• The Instagram login page will open. Enter the target’s
  • Instagram user name.
  • Don’t know the password, so tap ‘Get help signing in’.
• Select SMS option and enter your mobile number.
• You get the password link reset to your mobile phone
Social Media Hacks: Spyzie

- Spyzie is a monitoring solution for iOS and Android devices.
- Spyzie has a feature called Keylogger which allows you to record keystrokes typed by the person. It also sends the detailed report over to you through the internet.
- It allows you spy on the social network's history of someone including Instagram without figuring out the password as it also records this information.
- **Hacking Twitter** account you must install the app on the targets phone.
- Once installed you will have unrestricted access to the phone.
Social Media Hacks: TwitterHack

- TwitterHack is a site that allows you to hack a twitter account without installing Twitter.
- Go to http://twitterhacking.com/hack-twitter.
- Enter in the target’s Twitter Handle.
- The site produces Password Hash Codes as it’s performing several functions.
- At completion a message will appear noting the hack was successful.
- Click on the button to generate the password.
Social Media Hacks: Hoverwatch

- This app allows you to monitor each message sent and received in the target’s Facebook account.
- Hack Facebook as well as other social media accounts
- Give you access to all messages and calls
- Remain invisible while connected to accounts
- Can also use GPS tracking
- Front camera photo facility available
- Track phones even when target replaces SIM card
Know Thy Target

- **Reconnaissance:**
  - Information Gathering
    - Passive reconnaissance
      - Public records (all) and News Releases
    - Active reconnaissance
      - Calling help desk, daily routines, port scans and checking for flaws to produce errors.

- **Scanning and Enumeration:**
  - Scanning host, network and ports
  - Fingerprinting for software etc.

- **Final results provides:**
  - List of all machines on the network
  - Operating systems and Devices
  - System Administrator
  - Policies, Management and Administration of systems
Know Thy Target

• **Gaining Access:**
  - Network Attacks
    - Sniffing, Spoofing, Session Hijacking, DDOD, Man in The Middle
  - Host Attacks
    - Buffer overflow, Malware, SQL Injection, Adware
  - Mobile Attacks
    - Malware, Synchronization, Buffer Overflow, DOS, Phishing

• **Escalate Privileges:**
  - Dump Sam file
  - Retrieve passwords `/etc/passwd`
  - Kali – Armitage, Meterpreter or Emulator
  - Utilize DLL Preloading
Know Thy Target

- **Maintaining Access:***
  - Creating backdoors
  - Spyware
  - Hidings files
  - Rootkits
  - Steganography
  - Executing applications
    - Spyware
    - Trojans

- **Hide all Evidence:***
  - Delete logs
  - Disable auditing
  - Manipulate logs
## Top Passwords 2018

<table>
<thead>
<tr>
<th>Rank</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
</tr>
<tr>
<td>2</td>
<td>password</td>
</tr>
<tr>
<td>3</td>
<td>123456789</td>
</tr>
<tr>
<td>4</td>
<td>12345678</td>
</tr>
<tr>
<td>5</td>
<td>12345</td>
</tr>
<tr>
<td>6</td>
<td>111111</td>
</tr>
<tr>
<td>7</td>
<td>1234567</td>
</tr>
<tr>
<td>8</td>
<td>sunshine</td>
</tr>
<tr>
<td>9</td>
<td>qwerty</td>
</tr>
<tr>
<td>10</td>
<td>iloveyou</td>
</tr>
<tr>
<td>11</td>
<td>princess</td>
</tr>
<tr>
<td>12</td>
<td>admin</td>
</tr>
<tr>
<td>13</td>
<td>welcome</td>
</tr>
<tr>
<td>14</td>
<td>666666</td>
</tr>
<tr>
<td>15</td>
<td>abc123</td>
</tr>
<tr>
<td>16</td>
<td>football</td>
</tr>
<tr>
<td>17</td>
<td>123123</td>
</tr>
<tr>
<td>18</td>
<td>monkey</td>
</tr>
<tr>
<td>19</td>
<td>654321 New</td>
</tr>
<tr>
<td>20</td>
<td>!@#$%^&amp;*</td>
</tr>
<tr>
<td>21</td>
<td>charlie</td>
</tr>
<tr>
<td>22</td>
<td>aa123456</td>
</tr>
<tr>
<td>23</td>
<td>donald</td>
</tr>
<tr>
<td>24</td>
<td>password1</td>
</tr>
<tr>
<td>25</td>
<td>qwerty123</td>
</tr>
</tbody>
</table>
I’ve hacked you now what?

- Hijack your usernames and passwords
- Steal money from your accounts
- Open new accounts in your name
- Ruin your credit
- Request a new cards to your accounts
- Make purchases
- Be added to accounts as an authorized user
- Obtain cash advances
- Use and abuse your Social Security number
- Sell your information to other parties
Hacking in Progress.......
Women in IT/Cyber

• Dorothy E. Denning
  • Information security researcher
  • Lattice-Based Access Control (LBAC)
  • Real-time IDS
  • Model included 8 abnormal activities of behavior
  • 4 Books
  • Over 200 articles
  • Inducted into National Cyber Security Hall of Fame 2012
Women in IT/Cyber

• Theresa Payton
  • Cybersecurity and IT Strategy
  • Former White House CIO
• Books
  • Protecting Your Internet Identity: Are You Naked Online?
  • Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family
WIT (Women in Technology)

WIT focuses on advancing women in technology.

Programs offered:
- Girls in Technology
- Cyber Patriot
- Mentor-protégé
- Leadership Foundry
- Scholarships
Women in Technology (WIT)

WIT offers:

• Leadership development
• Technology education
• Networking and mentoring opportunities for women at all levels of their careers.

• More information can be found at:
• [https://www.womenintechnology.org/home](https://www.womenintechnology.org/home)
Women in cybersecurity (wicys)

- Launched in 2013
- Linking women in cybersecurity together to share knowledge/experience, networking and mentoring.
- Offers:
  - Scholarships
  - Research opportunities
  - Conference opportunities
  - Workshops
  - Career opportunities
  - Learning resources
  - [https://www.csc.tntech.edu/wicys/resources/](https://www.csc.tntech.edu/wicys/resources/)
Other Associations

• Women In Technology International: https://www.witi.com/

• Women’s society of cyberjutsu (WSc): http://womenscyberjutsu.org

• Geek Feminism Wiki: http://geekfeminism.wikia.com/wiki/Geek_Feminism_Wiki

• Women Who Code: https://www.womenwhocode.com

• Black Girls Who Code: http://www.blackgirlscode.com
Questions?
THANK YOU

Https://DuchessofCybersecurity.com

Dr. Chanel Suggs – Duchess of Cybersecurity®

DrSuggs@DuchessofCybersecurity.com