Protecting Your Online Accounts
Authentication

• First line of defense in cybersecurity!
• Identify
  • State you who are!
• Prove
  • Verify you own the identity
Online Identifiers

- Username
- E-mail Address
- Identification number
- Phone number
- IP Address
- Device fingerprints
- Cookies
Have I Been pwned?

https://haveibeenpwned.com/
What to do if your online identity has been compromised?

DON’T PANIC!

UPDATE YOUR PASSWORDS...OFTEN!

USE UNIQUE PASSWORDS

ENABLE 2-FACTOR AUTHENTICATION

DELETE OLD ACCOUNTS
Authentication Methods

- Something you know
  - Passwords
  - PIN Number
  - Passphrase

- Something you have
  - Smartphone
  - Smart card/ID card

- Something you are
  - Fingerprint
  - Facial Recognition
  - Eye Scan
Password Security

• Most often used method of authentication
  • Simple, inexpensive, and effective
  • Not full proof!
How passwords get compromised

• Shared with others
• Shoulder surfing/written in an accessible place
• Social Engineering
• Data Breaches
• Dictionary Attacks
• Brute Force Attacks
Creating A Strong Password

<table>
<thead>
<tr>
<th>Randomness</th>
<th>Length</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Avoid dictionary words and names</td>
<td>• The longer the password, the harder to crack</td>
<td>• More character options = more time to crack</td>
</tr>
</tbody>
</table>
# How Long Does It Take To Crack a Password

<table>
<thead>
<tr>
<th>Number of Characters</th>
<th>Numbers only</th>
<th>Upper or Lower case letters</th>
<th>Upper or Lower case letters mixed</th>
<th>Numbers, Upper &amp; Lower case letters</th>
<th>Numbers, Upper &amp; Lower case letters, Symbols</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>instantly</td>
<td>instantly</td>
<td>instantly</td>
<td>instantly</td>
<td>instantly</td>
</tr>
<tr>
<td>4</td>
<td>instantly</td>
<td>instantly</td>
<td>instantly</td>
<td>instantly</td>
<td>instantly</td>
</tr>
<tr>
<td>5</td>
<td>instantly</td>
<td>instantly</td>
<td>instantly</td>
<td>3 secs</td>
<td>10 secs</td>
</tr>
<tr>
<td>6</td>
<td>instantly</td>
<td>instantly</td>
<td>8 secs</td>
<td>3 mins</td>
<td>13 mins</td>
</tr>
<tr>
<td>7</td>
<td>instantly</td>
<td>instantly</td>
<td>5 mins</td>
<td>3 hours</td>
<td>17 hours</td>
</tr>
<tr>
<td>8</td>
<td>Instantly</td>
<td>13 mins</td>
<td>3 hours</td>
<td>10 days</td>
<td>57 days</td>
</tr>
<tr>
<td>9</td>
<td>4 secs</td>
<td>6 hours</td>
<td>4 days</td>
<td>1 year</td>
<td>12 years</td>
</tr>
<tr>
<td>10</td>
<td>40 secs</td>
<td>6 days</td>
<td>169 days</td>
<td>106 years</td>
<td>928 years</td>
</tr>
<tr>
<td>11</td>
<td>6 mins</td>
<td>169 days</td>
<td>16 years</td>
<td>6k years</td>
<td>71k years</td>
</tr>
<tr>
<td>12</td>
<td>1 hour</td>
<td>12 years</td>
<td>600 years</td>
<td>108k years</td>
<td>5m years</td>
</tr>
<tr>
<td>13</td>
<td>11 hours</td>
<td>314 years</td>
<td>21k years</td>
<td>25m years</td>
<td>423m years</td>
</tr>
<tr>
<td>14</td>
<td>4 days</td>
<td>8k years</td>
<td>778k years</td>
<td>1bn years</td>
<td>5bn years</td>
</tr>
<tr>
<td>15</td>
<td>46 days</td>
<td>212k years</td>
<td>28m years</td>
<td>97bn years</td>
<td>2tn years</td>
</tr>
<tr>
<td>16</td>
<td>1 year</td>
<td>512m years</td>
<td>1bn years</td>
<td>6tn years</td>
<td>193tn years</td>
</tr>
<tr>
<td>17</td>
<td>12 years</td>
<td>143m years</td>
<td>36bn years</td>
<td>374tn years</td>
<td>14qd years</td>
</tr>
<tr>
<td>18</td>
<td>126 years</td>
<td>3bn years</td>
<td>1tn years</td>
<td>23qd years</td>
<td>1 qt years</td>
</tr>
</tbody>
</table>
Strong and Easy Passwords

The Sun Will Come Out, Tomorrow, Bet Your Bottom Dollar

tswcotbybd  Random!
tswco)t(bybd  12 Characters + Symbols!
TsWc0)t(ByBd  Mixed case and numbers!
a$TsWc0)t(ByBd  Add “a$” for Amazon.com
emTsWc0)t(ByBd  Add “em” for email
Password Managers

**Pros**
- Ease of use
- Strong, random password creation
- Encrypted storage
- 2-factor Authentication
- May include other benefits and features

**Cons**
- Have cost associated with use
- “Putting all your eggs in one basket”
- Password manager breach
- Forgetting your master password
- Setup time
Password Do’s and Don’ts

• Don’t write it down!
  • If you do, keep it in a secure place
• Don’t store passwords in programs
  • Browser/Website
  • Save login
• Don’t tell anyone for any reason
  • Not to family
  • Not to the IT Person
  • Not to anyone on the phone
• Change your password from time to time
  • Secure passwords can be compromised
  • Recommended every 90-180 days
Multifactor Authentication

- Using two or more methods to authenticate
  - Something you know
  - Something you have
  - Something you are
- Adds an extra layer and an extra step
  - Makes it harder for an attacker to access your account
  - Less convenient for you
Common Multifactor Authentication Types

Challenge Questions
- Technically not multifactor
- Challenge answers can be discovered through social engineering

SMS (Text message) Token Authentication
- Password or code sent to your phone
- Messages are time sensitive and could be delayed
- Maybe be vulnerable to attacks (SIM Swapping)

Authenticator Apps
- App installed on your phone. Click approve or get a code
- Loss or change of phone may cause issues
- Lack of support/different apps for different sites
Less Common Multifactor Authentication Types

• Hardware based one time password
  • Code is randomly generated on a hardware “key”
  • Expensive to implement and not widely used

• Smartcards and cryptographic hardware tokens
  • Card or device that stores keys to authenticate user
  • Expensive to implement and not widely used