Cybersecurity: A Big Concern for Small Fish

Jim Peterson, IT Manager
Simpson County Library District
Franklin, KY
Everything is vulnerable to some point!

- Computers – laptops, desktops & servers
- Devices – phones, tablets, Nintendo DS
- IoT devices – thermostats, A/C controllers
- Network equipment – switches & routers
- Software Applications
- Operating Systems
IoT Devices Make Sense for Libraries

Easy to monitor and adjust for utility cost savings

Can be remotely monitored by staff or an outside service

Little to no burden on existing staff

What is IoT?

IoT, the “Internet of Things,” is a term that describes a network of physical objects connected to the internet. These may be discrete items like light bulbs or larger systems like building automation solutions. Embedded in each device are electronics capable of network connectivity along with sensors or other features.
Cyber attacks come from EVERYWHERE!!
What Do They Want and Why??

addresses
socials
emails
credit cards
passwords
birthdays
Not Just Personal Information

1. Hardware and Bandwidth
   a. building botnets
   b. serving spam

2. Mischievous Purposes
   a. Deface/Defame
   b. Hosting porn/malware
Social Engineering paves the way!

Ransomware  Phishing

Worms & Trojans

It all starts with an exploit kit...
What Phishing Is and How It Works

**Phishing**

1. Build fake site.
2. Victims click on link in email believing it is legitimate. They enter personal information.
3. Fraudsters compile the stolen data and sell it online or use it themselves.

**Why Phishing Scams Keep Working**

**Wait for It**

**There It Is**

- Enter your bank account number.
  - SCAM.
- Enter your bank account number.
  - SCAM.
- Enter your bank account number.
  - OKEY-DOKEY.
Your computer has been locked due to suspicion of illegal content downloading and distribution.

Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A- Certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

Technical details:
Involved IP address: [Redacted]
Involved host name: http://pornerbros.com

How to unlock your computer:

1. Take your cash to one of this retail locations:
   - Walmart
   - CVSpharmacy
   - Walgreens

2. Get a MoneyPak and purchase it with cash at the register

3. Come back and enter your MoneyPak code to unlock your computer (6 attempts available)

In order to resolve the situation in an above-mentioned way you should pay a fine of $300.

Permanent lock on 05/01/2013 5:20 p.m. EST
**LET’S DO SOME MATH**

- **Number of users redirected daily**: 20,000
- **A typical success rate of Exploit Kits**: 10%
- **Percentage of victims to pay ransom**: 0.5%
- **Daily income**: 
  \[20,000 \times 10\% \times 0.5\% \times $300 = $3,000\]
- **Monthly income**: $90,000

- **Net monthly income**: 
  \[$90,000 - $5,900^* = $84,100\]

*Assumes $5,900 for a custom malware payload*
There’s NO Stopping the Attacks, but...
**Worst Passwords of 2016**

SplashData releases its annual list in an effort to encourage the adoption of stronger passwords to improve Internet security. The passwords evaluated are mostly from North American and Western European users. The list shows many people continue to put themselves at risk for hacking and identity theft by using weak, easily guessable passwords.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Password</th>
<th>Change from 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td>Unchanged</td>
</tr>
<tr>
<td>2</td>
<td>password</td>
<td>Unchanged</td>
</tr>
<tr>
<td>3</td>
<td>12345</td>
<td>↑</td>
</tr>
<tr>
<td>4</td>
<td>12345678</td>
<td>↑</td>
</tr>
<tr>
<td>5</td>
<td>football</td>
<td>↑</td>
</tr>
<tr>
<td>6</td>
<td>qwerty</td>
<td>↑</td>
</tr>
<tr>
<td>7</td>
<td>123456789</td>
<td>↑</td>
</tr>
<tr>
<td>8</td>
<td>1234567</td>
<td>↑</td>
</tr>
<tr>
<td>9</td>
<td>princess</td>
<td>↑</td>
</tr>
<tr>
<td>10</td>
<td>login</td>
<td>↑</td>
</tr>
<tr>
<td>11</td>
<td>welcome</td>
<td>↓</td>
</tr>
<tr>
<td>12</td>
<td>solo</td>
<td>↑</td>
</tr>
<tr>
<td>13</td>
<td>abc123</td>
<td>↑</td>
</tr>
<tr>
<td>14</td>
<td>admin</td>
<td>↑</td>
</tr>
<tr>
<td>15</td>
<td>121212</td>
<td>↑</td>
</tr>
<tr>
<td>16</td>
<td>flower</td>
<td>↑</td>
</tr>
<tr>
<td>17</td>
<td>password</td>
<td>↑</td>
</tr>
<tr>
<td>18</td>
<td>dragon</td>
<td>↑</td>
</tr>
<tr>
<td>19</td>
<td>sunshine</td>
<td>↑</td>
</tr>
<tr>
<td>20</td>
<td>master</td>
<td>↑</td>
</tr>
<tr>
<td>21</td>
<td>hottie</td>
<td>↑</td>
</tr>
<tr>
<td>22</td>
<td>lovenme</td>
<td>↑</td>
</tr>
<tr>
<td>23</td>
<td>zaq1zaq1</td>
<td>↑</td>
</tr>
<tr>
<td>24</td>
<td>password1</td>
<td>↑</td>
</tr>
</tbody>
</table>

The 2016 list is based on over 5 million passwords posted or for sale on the Internet.

“123456” and “password” remain #1 and #2 for third straight year.

Almost 4% of people use the worst password, 123456.

Just over 10% of people use one of the 25 worst passwords.

“Hottie” and “lovenme” and “flower” make their first appearances on the SplashData list.

“Princess” and “solo” keep the Force from Star Wars going for another year.

Three variations of “password” on the list -- “password”, “password,” and “passwords”.

“We have seen an effort by many people to be more secure by adding characters to passwords, but if these longer passwords are based on simple patterns they will put you in just as much risk of having your identity stolen by hackers.”

Morgan Stain, CEO of SplashData
The Best Defense is a Strong Passphrase!!!

i shall use strong passwords.
i shall use strong passwords.
i shall use strong passwords.
i shall use strong passwords.
i shall use strong passwords.
I 5ha!! u53 $4rong-p@5sw0rdz!

Strong passwords are a minimum of 8 characters in length & include uppercase, lowercase, numbers & special characters.
It's a Much Different World Today, and It Will Be Even More So Tomorrow, Even in Libraries...

Smart Devices will become more ubiquitous:
Amazon Echo/Google Home
Wireless Thermostats
Irrigation controllers (sprinkler timers)
Smart Vents
Lighting
Electrical Outlets
Appliances both large & small
Locks
Jim Peterson
IT Manager, Goodnight Memorial Library
203 S Main St.
Franklin, KY 42134
(270) 586-8397
jim@gmpl.org

On Facebook
Twitter: @GMLGeek
Instagram: jimmythegeek71