Topics Today

- SECURITY THREATS
  - Who wants personal data?
  - How does data move on the Internet?
  - Where and how is data vulnerable?

- PASSWORD PROTECTION

- PRIVACY TOOLS
SECURITY
THREATS
Who wants personal data?

COMPANIES: advertising

GOVERNMENT: investigations

INDIVIDUALS: fraud
Who wants personal data?

COMPANIES: advertising

GOVERNMENT: investigations

INDIVIDUALS: fraud
How does data move through the Internet?

The Internet works by chopping data into chunks called packets. Each packet then moves through the network in a series of hops.

1. Sender
2. Wireless router
3. Modem
4. Entering the network

Each packet hops to a local Internet service provider (ISP), a company that offers access to the network – usually for a fee.

Inside library, office, café, etc.

CenturyLink, Mediacom, Spectrum, etc.

IMAGE CREDIT: Lazaro Gamio, Washington Post
How is data vulnerable?

The Internet works by chopping data into chunks called packets. Each packet then moves through the network in a series of hops.

CenturyLink, Mediacom, Spectrum, etc.

“THE INTERNET”

IMAGE CREDIT: Lazaro Gamio, Washington Post
While it may sound odd to worry about bad guys snatching our personal information from what seems to be thin air, it’s more common than we’d like to believe. In fact, there are hackers who drive around searching for unsecured wireless connections (networks) using a wireless laptop and portable global positioning system (GPS) with the sole purpose of stealing your information.
Wardriving

WiFi security = password-protected connection
We want open WiFi! Consider practical threats. We *can* educate patrons about security practices, strong passwords, etc.

**Remember:** “wired” connections (e.g. patron PCs) are quite secure; having a program to clear data upon each log-out even more so. *In your library?*
How is data vulnerable?

The Internet works by chopping data into chunks called packets. Each packet then moves through the network in a series of hops.

Access point

Entering the network

Each packet hops to a local Internet service provider (ISP), a company that offers access to the network — usually for a fee.

Activity

“THE INTERNET”

IMAGE CREDIT: Lazaro Gamio, Washington Post
"E-vesdropping"

Sender

Account name
Password
Social Security #

Spy

Server
Encryption over the Web

Hyper-Text Transfer Protocol Secure
Encryption over the Web

Sender

...11039225900287...
...65342003154354...
...92135892439243...

Server

?
What’s a library to do?

Use links to HTTPS websites whenever possible

Keep all software updated!
E-mail encryption

E-mail uses dedicated "protocol" requiring different encryption; also limited by correspondents’ platform

Options:
- Settings within popular services (Gmail, Outlook, Yahoo)
- Dedicated service (ProtonMail, Hushmail)
How is data vulnerable?

The Internet works by chopping data into chunks called packets. Each packet then moves through the network in a series of hops.

1. **Wireless router**
2. **Modem**
3. **Entering the network**
   - Each packet hops to a local Internet service provider (ISP), a company that offers access to the network—usually for a fee.

**IMAGE CREDIT:** Lazaro Gamio, Washington Post

“THE INTERNET”

human behavior
Phishing

Merriam-Webster.com: “a scam by which an Internet user is duped (as by a deceptive e-mail message) into revealing personal or confidential information which the scammer can use illicitly”
CSO Online: 15 real-world phishing examples

Phishing Scenario: Look-Alike Websites
Don’t take the bait!

Do you recognize sender’s email address?

Look at link URLs before clicking — https://www.website-you-want.com?

Suspicious? Don’t click, contact IT!
PHISHING SCENARIO: Deactivation Scares

Dear [email],

Recently, there's been activity in your account that seems unusual compared to your normal account activities.

This is detail your activity:
- Location: 38 Paralola Street, Cebu, Philippines
- IP Address: 74.77.65.14 (74.77.65.14 uten.net)
- Time: Thursday, 12 October 2017, 03:37:50 PM

If you do not do this activity, maybe someone who has access your account. To view the details of your case please download & read Billing_Agreement_11192017.pdf in attachment.

PHISHING SCENARIO: Tech Support Scams

- Your Facebook, Skype, AIM, ICQ and other chat logs
- Your private & family photos and other sensitive files
- Your webcam could be accessed remotely by hackers

IMMEDIATELY CALL MICROSOFT CERTIFIED TECHNICIANS AT 1-855-767-7669

MORE ABOUT THIS INFECTION:

Seeing these pop-ups means that you have a virus installed on your computer which runs the security of your personal data at a serious risk.

It's strongly advisable that you call the number above and get your computer inspected before you continue using your Internet, especially for Shopping or Banking.

Call immediately for urgent assistance. Contact Microsoft Certified Technicians at 1-855-767-7669.

PHISHING SCENARIO: Go Directly to Jail

You have been subjected to violations of Copyright in the Criminal Code of United States of America. Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law on Negligent Use of Personal Computer. Article 210 of the Code provides for a fine of up to $100,000 and/or deprivation of liberty for four to nine years.

Pursuant to the amendment to Criminal Code of United States of America May 28, 2011, this law enforcement (if it is not repeated - first time) may be considered as conditional in case you pay the fine of the States.

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $300. Payable through ClearOut MoneyPak (you have to purchase MoneyPak card, load it with $300 and enter the code). You can buy the code at any shop or gas station.

PHISHING SCENARIO: Save a Friend

[Image of a wallet]
How is data vulnerable?

The Internet works by chopping data into chunks called packets. Each packet then moves through the network in a series of hops.

**Sender**

1. **Wireless router**

2. **Modem**

3. **Entering the network**
   - Each packet hops to a local Internet service provider (ISP), a company that offers access to the network—usually for a fee.

**Image Credit:** Lazaro Gamio, Washington Post
Data breaches

The Equifax Data Breach: What to Do

September 8, 2017
by Seena Gressin
Attorney, Division of Consumer & Business Education, FTC

If you have a credit report, there’s a good chance that you’re one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation’s three major credit reporting agencies.
Data breaches

Stay informed with
Federal Trade Commission
Consumer Information blog:

https://www.consumer.ftc.gov/blog
PASSWORD PROTECTION
## GOAL: strong passwords

### 25 Of The Most Popular Passwords

<p>| | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td>2</td>
<td>password</td>
<td>3</td>
<td>12345678</td>
<td>4</td>
<td>qwerty</td>
</tr>
<tr>
<td>6</td>
<td>123456789</td>
<td>7</td>
<td>letmein</td>
<td>8</td>
<td>1234567</td>
<td>9</td>
<td>football</td>
</tr>
<tr>
<td>11</td>
<td>admin</td>
<td>12</td>
<td>welcome</td>
<td>13</td>
<td>monkey</td>
<td>14</td>
<td>login</td>
</tr>
<tr>
<td>16</td>
<td>starwars</td>
<td>17</td>
<td>123123</td>
<td>18</td>
<td>dragon</td>
<td>19</td>
<td>passw0rd</td>
</tr>
<tr>
<td>21</td>
<td>hello</td>
<td>22</td>
<td>freedom</td>
<td>23</td>
<td>whatever</td>
<td>24</td>
<td>qazwsx</td>
</tr>
<tr>
<td>20</td>
<td>master</td>
<td>25</td>
<td>trustno1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


GOAL: strong passwords

<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>12345678</td>
</tr>
<tr>
<td>4</td>
<td>qwerty</td>
</tr>
<tr>
<td>5</td>
<td>12345</td>
</tr>
<tr>
<td>6</td>
<td>123456789</td>
</tr>
<tr>
<td>7</td>
<td>letmein</td>
</tr>
<tr>
<td>8</td>
<td>1234567</td>
</tr>
<tr>
<td>9</td>
<td>football</td>
</tr>
<tr>
<td>10</td>
<td>iloveyou</td>
</tr>
<tr>
<td>11</td>
<td>abcn123</td>
</tr>
<tr>
<td>12</td>
<td>login</td>
</tr>
<tr>
<td>13</td>
<td>password</td>
</tr>
<tr>
<td>14</td>
<td>starwars</td>
</tr>
<tr>
<td>15</td>
<td>master</td>
</tr>
<tr>
<td>16</td>
<td>123123</td>
</tr>
<tr>
<td>17</td>
<td>dragon</td>
</tr>
<tr>
<td>18</td>
<td>whatever</td>
</tr>
<tr>
<td>19</td>
<td>qazwsx</td>
</tr>
<tr>
<td>20</td>
<td>master</td>
</tr>
<tr>
<td>21</td>
<td>hello</td>
</tr>
<tr>
<td>22</td>
<td>freedom</td>
</tr>
<tr>
<td>23</td>
<td>whatever</td>
</tr>
<tr>
<td>24</td>
<td>qazwsx</td>
</tr>
<tr>
<td>25</td>
<td>trustno1</td>
</tr>
</tbody>
</table>
GOAL: strong passwords

Current guidelines to avoid being easily guessed by humans or robots...

- 12-15 characters
- No dictionary words
- No obvious details (name, phone #, etc.)
- Different for each account
- Change if any suspicion!
GOAL: strong passwords

Turn a memorable phrase into secure password...

Example:
“Be happy for this moment; this moment is your life”
Bh4tm;tmiyl5433 (15 characters)
GOAL: password security

Not in plain sight! (no sticky notes on monitors)

Best practice: stored only in staff brains, with knowledge of how to reset them
GOAL: patron protection

From ALA’s Privacy Tool Kit:

“Confidentiality of library records is a core value of librarianship...For libraries to flourish as centers for uninhibited access to information, librarians must stand behind their users’ right to privacy and freedom of inquiry.”
PRIVACY
TOOLS
Who wants personal data?
Game Day Data Package
Plan your winning strategy with the best consumer data package in the game. We open our playbook to help you reach sports fans.

Valentine’s Day Data Package
Forbes called it “America’s $20 Billion Day of Love,” and Acxiom can introduce you to this seasonal audience of your dreams – gift givers and big spenders.

Mother’s Day Data Package
Using audience insights, Acxiom can help you target your ideal digital audience for this mother of all marketing opportunities.

Summer Fun Data Package
As temperatures heat up, so does your opportunity to reach seasonal audiences through Acxiom’s data packages. Connect to vacationers, campers, boaters, beach goers and other active digital audiences.
Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser

Privacy Settlement is the Largest FTC Penalty Ever for Violation of a Commission Order
FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook

FTC settlement imposes historic penalty, and significant requirements to boost accountability and transparency
Slate: Facebook, Inc. expects 2019 earnings of $69 billion

2019 documentary investigating U.K. digital marketing firm Cambridge Analytica and targeted social media advertising campaigns in political elections worldwide

Directed by Karim Amer and Jehane Noujaim
“Filter bubble”

Merriam-Webster.com: “an online environment in which people are exposed only to opinions and information that conform to their existing beliefs”

Fun experiment: Try same keywords in different search engines on various computers
“Anonymize” your ads

Facebook:
https://www.facebook.com/ads/preferences

Google:
https://support.google.com/ads/answer/2662922
DuckDuckGo

Free “privacy-dedicated search engine that does not collect or share personal information” such as search terms, location, etc.

https://duckduckgo.com
“Private” browsing modes

- Chrome privacy settings: Incognito window
- Firefox privacy settings: Private window
- Internet Explorer settings: InPrivate window
- Safari privacy settings: Private window
Browser add-ons

**Ghostery**
“control over ads and tracking technologies”

**Privacy Badger**
“block invisible trackers”
More privacy tools and info

Library Freedom Project:
https://www.libraryfreedom.org

Electronic Frontier Foundation:
https://www.eff.org