Security Risks on Apps and Websites

In This Module

- What are some of the risks and pitfalls that can exist on apps and websites?
- How can you avoid security risks on apps and websites?

Security Risks on Apps and Websites

Unsecured and risky apps and websites can carry a number of different security pitfalls that can put your personal data and information at risk, including trackers and malware

Risky Apps and Websites

- **Malware:** These sites might contain malware that can track your activity or install things like viruses or spyware on your machine
- **Data risks:** These sites might put your personal data at risk with poor data storage practices
- **Unsecured logins:** These sites might use poor practices for logins, which puts your security at risk
- **Trackers and cookies:** These sites might expose you to invasive, third-party trackers and cookies

What Are Signs of a Risky Site or App?

- Sites or apps that have free downloads of software or movies
- Sites that ask for your personal and banking information when it doesn't seem necessary
- Apps that request excessive permissions
- Sites with suspicious looking URLs or URLs that don't have an "https"

How Can You Avoid Risky Apps?

- Install apps from recognized and legitimate sources, like your phone's app store
- Do research before you install anything on your device
- Pay attention to permissions
  - Make sure you understand what the app is doing
  - Make sure you are comfortable with the permissions the app is requesting

How Can You Avoid Risky Websites?

- Use a safe search mode to filter out explicit results
- Search for websites rather than trying to type in the URL
- Pay attention to warnings from your browser

How Can You Avoid Risky Websites?

- Double check the URL
- Avoid clicking suspicious links
- Check shortened links with a URL expander
  - CheckShortURL
  - Expand URL
- Make sure the site you are visiting has an “https” in the URL

Takeaways

- Apps and websites can carry a number of risks, including malware and poor data storage practices
- Sites or apps that offer your suspicious things (like free downloads of paid software) or that ask for an excessive amount of personal information should be treated with caution and avoided
- Being alert and aware of the types of apps and sites you are visiting and engaging with can help you avoid getting exposed to malware or having your data compromised

Resources

The Electronic Frontier Foundation's Surveillance Self-Defense Guide (link)

"Protect Your Privacy From the Apps on Your Phone" from *Consumer Reports* (link)

"How to Clear Your Cache on Any Browser" from *PC Mag* (link)

Swiss Cyber Institute's Guide to Safe Web Browsing (link)

Questions?

NYC Digital Safety

Privacy & Security