Topic 5 Discussion 1

There is hardly a week without news of ransomware attacks or data breaches. Outline five best practices individuals should adopt to protect their digital assets and information. What are the effects of the internet and social media on privacy?

Hello Class,

Five Best Practices for Protecting Digital Assets and Information:

**Strong Passwords and Multi-Factor Authentication (MFA)** - Use unique, complex passwords for each online account and enable MFA whenever possible. MFA adds an extra layer of security by requiring a second form of verification, such as a code sent to your phone, beyond just your password(NIST, 2024).

**Software Updates and Security Patches** - Keep your operating systems, applications, and antivirus software up-to-date. Software updates often include security patches that fix vulnerabilities that hackers could exploit.

**Secure Wi-Fi Networks** - Avoid using public Wi-Fi for sensitive transactions, such as online banking. If you must use public Wi-Fi, consider using a VPN (Virtual Private Network) to encrypt your internet traffic(FTC, 2018).

**Phishing and Social Engineering Awareness** - Be cautious of suspicious emails, messages, or phone calls. Never click on links or open attachments from unknown senders. Legitimate organizations will rarely ask for personal information via email or text(CISA, 2025).

**Regular Backups** - Regularly back up your important files to an external hard drive, cloud storage, or other secure location. This protects your data in case of a device failure, ransomware attack, or other data loss event.

Effects of the Internet and Social Media on Privacy

The internet and social media have profoundly impacted privacy. The ease of data collection and sharing online means that vast amounts of personal information are constantly being gathered, often without our full knowledge or consent. Social media platforms, in particular, track user activity, collect personal data, and often share this data with third-party advertisers and other entities. This can lead to targeted advertising, but also raises concerns about data security and the potential for misuse of personal information(Privacy Alliance, 2025). The lack of transparency in data collection practices and the difficulty in controlling how our data is used are significant challenges to privacy in the digital age. Furthermore, the permanence of online information means that things posted online can remain accessible for years, potentially impacting an individual's reputation and opportunities.

References:

CISA. (2025). *Cybersecurity Best Practices*. Www.cisa.gov. https://www.cisa.gov/topics/cybersecurity-best-practices

FTC. (2018, October 31). *Report Identity Theft*. Federal Trade Commission. https://www.ftc.gov/news-events/topics/identity-theft/report-identity-theft

NIST. (2024). *Cybersecurity Framework*. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

Privacy Alliance. (2025). *Privacy Alliance*. Privacyalliance.org. https://www.privacyalliance.org