Contents

Overview

With the increasing use and reliance on digital platforms, organizations and individuals are becoming more exposed to various cybersecurity risks. Malicious on-line activity exploits security vulnerabilities to collect personal data, disrupt or deny service and degrade information technology resources. According to a 2023 report from Forbes, there was a 72% increase in data breaches since 2021. An astounding 94% of organizations report e-mail security incidents, with malware being the most common issue.

The Federal Communications Commission notes, “Recent information shows that such schools and libraries are vulnerable to increased cybersecurity threats and attacks, often leading to the disruption of school and library operations, loss of learning, reductions in available bandwidth, significant monetary losses, and the leaking and theft of students’, school staff members, and library patrons’ personal information and confidential data.”

With the growing threat of financial fraud, unauthorized access, and identity theft, it is important that local libraries undertake cybersecurity measures. Cybersecurity encompasses the technology, practices and safety measures used to safeguard computer networks against unauthorized access and to protect the confidentiality, integrity and availability of the data house on these networks.

State and Federal Initiatives

Montana State Information and Technology Services Division (SITSD)

The Montana State Information and Technology Services Division (STITSD) has a cybersecurity office that is responsible for increasing awareness through activities such as "Cybersecurity Month" (October). The office maintains a website with links to cybersecurity resources for local governments, non-profits, businesses and individuals. The website also includes information for reporting cybersecurity incidents.

- MT SITSD Cybersecurity webpage

Montana Digital Opportunity Plan

In 2022, the Montana State Broadband Office (https://connectmt.mt.gov/) received a grant from the federal Digital Equity Act. The plan will be the basis for funding implementation activities identified in the plan.

Cyber-security is one of the six goals in the Digital Opportunity Plan.

- Online privacy and cyber-security: Ensure all Montana residents have access to high-speed internet that meets online privacy and cybersecurity standards.

U.S. Cybersecurity Infrastructure Security Agency (CISA)

CISA is a division within the U.S. Department of Homeland Security. It was established in 2018 as the nation's cyber defense agency and is charged with helping organizations prepare for, respond to, and mitigate the impact of cyberattacks.

The agency website includes cybersecurity alerts, resources, training programs and other tools for both large and small local governments, businesses and other organizations.

- CISA Cybersecurity Best Practices

Best Practices

Libraries have dual cybersecurity concerns. Not only do they need to protect their computer systems against cyber threats, but libraries have patrons using public access computers and free wi-fi that can also compromise a library's network. Increasing awareness among staff and patrons of cybersecurity best practices is the first and foremost line of defense. Following are tips for being cybersmart.

Libraries

- Install anti-virus software on all devices. Anti-virus software can automatically detect and remove many types of malware. Enable updates and scans for maximum security against latest threats.
- Keep software up-to-date (especially operating systems) to fix potential vulnerabilities that hackers may try to exploit.
- Utilize a firewall to prevent attacks and to limit malicious traffic before it compromises the network. Some devices, routers and operating systems include a firewall.
- Regularly back-up critical data.
- Develop a cybersecurity plan to identify and fix security flaws and establish cybersecurity policies. Include a response plan in case of a cybersecurity incident.
- Report cyberattacks and scams to appropriate agencies. Post fraud alerts for patrons.
    - Montana SITSD Cybersecurity Reporting Site
- Coordinate with Internet providers and IT staff at city and county governments to implement cybersecurity measures.
- Train staff on cybersecurity threats and precautionary measures. (See CISA website for on-line training.) Attend cybersecurity workshops at conferences and share information with peers.

Staff/End-Users/Patrons

- Passwords - Use strong passwords that will be difficult for cybercriminals to guess. Use different passwords for different devices and accounts. Don't share your passwords and usernames.
- Enable multi-factor authentication (i.e. two-step login process) to ensure that the patron/end-user is the only person who has access to their account.
- Avoid clicking on untrustworthy links or downloading software from unknown sources. Check URL's for unusual characters, misspellings, or other suspicious words that could indicate it is a fake website. Don't automatically click on links – Stop & think about it before you connect to a new site.
- Recognize common scams and cybersecurity threats. Report scams and suspicious activities to appropriate government agencies
    - MT SITSD Cybersecurity Reporting Site
- Manage privacy settings on social media. Don't "friend" people you don't know. Report, block or hide any person that is making you feel uncomfortable on-line. Be careful posting personal info.
- When banking and shopping, check if the site is security enabled. Addresses with **"https://"** or **"shttp://,"** means the site takes extra measures to help secure your information. "Http://" is not secure. Avoid making business transactions on public access computers or public wi-fi.

- Links in emails, social media posts and online advertising are often how cybercriminals try to steal personal information. Even if you know the source, if something looks suspicious, delete it.
- Think before you act: Be wary of communications that implore you to act immediately, offer something that sounds too good to be true or ask for personal information.
- Back it up: Protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely.

Glossary

Term	Definition
Malware	Malware is any software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
Phishing	The process of scammers tricking you into giving them your personal information.
Ransom Ware	A type of malware that holds a victim's data for ransom.
Social Engineering Fraud	Social engineering fraud refers to scams used by criminals to exploit a person's trust in order to obtain money or obtain confidential information.
Hacking	Hacking occurs when an unauthorized user gets access to your device or account. Hackers can steal your identity to make unauthorized purchases, spam your contacts or engage in other malicious activities.
Identify Theft	Identity theft happens when someone takes your name and personal information (i.e. social security number) and uses it without your permission to do things like open new accounts, use your existing accounts, or obtain medical services.
Denial of Service	A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to malware or hacking.
Scams	An online scam is a deception carried out over the internet with the aim of tricking individuals into giving away personal, financial, or other sensitive information, or directly stealing their money. For more info on latest scams visit AARP About Fraud Watch Network webpage.

Resources

Agencies

Federal Communications Commission

- https://www.fcc.gov/cybersecurity-pilot-program

Montana State Information and Technology Services Division

- https://sitsd.mt.gov/Cybersecurity/
- https://sitsd.mt.gov/Cybersecurity/Reporting

Montana Broadband Office, “Montana Digital Opportunity Plan”

- https://connectmt.mt.gov

U.S. Cybersecurity Infrastructure Security Agency (CISA)

- https://www.cisa.gov/topics/cybersecurity-best-practices
- https://www.cisa.gov/online-toolkit-partnering-safeguard-k-12-organizations-cybersecurity-threats

Articles

- Forbes Advisor Cybersecurity Facts and Figures, 2023
- Ransomware Attacks at Libraries: How They Happen, What to Do
- Cyber.org
- Stay Safe Online
- Reasonable Cybersecurity Guide
- About AARP Fraud Watch Network