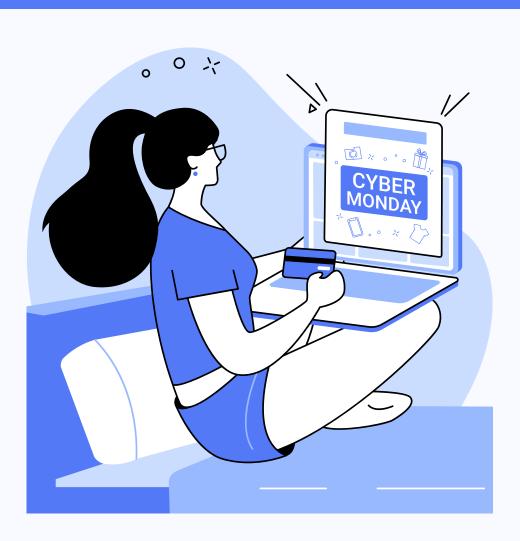# CYBERSECURITY

Cyberattacks are malicious attempts to access or damage a computer or network system. Cyberattacks can lead to the loss of money or the theft of personal, financial and medical information.

These attacks can damage your reputation and safety. Cybersecurity involves preventing, detecting and responding to those cyberattacks that can have wide-ranging effects on individuals, organizations, the community and the nation.

CYBER MONDAY

YOU CAN AVOID CYBER RISKS BY TAKING STEPS IN ADVANCE:

- **Limit the personal information you share online. Change privacy settings and do not use location features.**

- **Keep software applications and operating systems up-to-date.**

- **Create strong passwords by using upper and lower case letters, numbers and special characters. Use a password manager and two methods of verification.**

- **Watch for suspicious activity that asks you to do something right away, offers something that sounds too good to be true, or needs your personal information. Think before you click. When in doubt, do NOT click.**

- **Be cautious about sharing personal financial information, such as your bank account number, Social Security number or credit card number. Only share personal information on secure sites that begin with https://. Do not use sites with invalid certificates. Use a Virtual Private Network (VPN) that creates a more secure connection.**

- **Do not click on links in texts or emails from people you don't know. Scammers can create fake links to websites.**

DURING A CYBERATTACK

- Check your credit card and bank statements for unrecognizable charges.

- Check your credit reports for any new accounts or loans you didn't open.

- Be alert for emails and social media users that ask for private information.

- If you notice strange activity, limit the damage by changing all of your internet account passwords immediately.

- Let work, school or other system owners know what happened.

- **Contact banks, credit card companies and other financial services companies where you hold accounts. You may need to place holds on accounts that have been attacked. Close any unauthorized credit or charge accounts. Report that someone may be using your identity.**

- **File a report with the [Office of the Inspector General (OIG)](#) if you think someone is using your Social Security number illegally.**

- **Report identity theft to the [Federal Trade Commission](#). Contact the Federal Trade Commission (FTC) at [ftc.gov/complaint](#) if you receive messages from anyone claiming to be a government agent.**

- **Contact additional agencies depending on what information was stolen.**