CYBERSECURITY 101

At home or at work, our growing dependence on technology demands greater security online. Individuals are our community’s first line of defense in guarding against online risks. For this reason, cybersecurity is a shared responsibility, requiring awareness and vigilance from every citizen, community, and country.

The Salt Lake Chamber is partnering with the Stop.Think.Connect.TM Campaign, a national public awareness effort to guide the nation to a higher level of Internet safety by challenging Utahns to be more vigilant about practicing safer online habits.

To understand and practice cybersecurity, individuals must be able to recognize risks, threats, and vulnerabilities that exist online and their impact at a national and individual level.

CYBER RISKS

WHO
Malicious actors intend to cause harm in cyberspace, such as a hacker stealing personal information. Benign actors accidentally cause harm to a network, system, or the Internet, such as an employee who accidentally downloads malware onto their company’s network.

WHAT
Malicious actors exploit the anonymity and vulnerabilities of the Internet using methods that range in sophistication from botnets to viruses. Benign actors introduce threats through simple actions that can range from clicking on an unknown link to using a USB drive.

WHEN
It is impossible to predict when a cyber incident will occur. Keep alert of possible warning signs of an intrusion.

WHERE
Cyberspace, often interchanged with “the Internet,” is created by and accessible through computer networks that share information and facilitate communication. Unlike the physical world, cyberspace has no boundaries across air, land, sea, and space.

WHY
Benign actors unintentionally and often unknowingly cause harm while malicious actors may have a range of motives, including seeking confidential information, money, credit, prestige, or revenge.

There are many risks online, some more serious than others. The majority of cybercriminals are indiscriminate; they target vulnerable computer systems regardless of whether they are part of a government agency, Fortune 500 company, a small business, or belong to a home user.

CYBER TIPS

No citizen, business, community, or country is immune to cyber risk, but there are steps you can take to minimize your chances of experiencing a cyber incident:

- Set strong passwords, change them regularly, and don’t share them with anyone.
- Keep your operating system, browser, and other critical software optimized by installing updates.
- Maintain an open dialogue with your friends, family, and colleagues about Internet safety.
- Use privacy settings and limit the amount of personal information you post online.
- Be cautious about offers online—if it sounds too good to be true, it probably is.

CYBER INCIDENT RESPONSE

Take Immediate Action. The extent, nature, and timing of cyber incidents are impossible to predict. There may or may not be any warning. Some cyber incidents take a long time (weeks, months, or years) to be discovered and identified. If you are a victim of a cyber incident, follow the steps below to mitigate and recover from the incident.

IMMEDIATE ACTIONS

- Check to make sure the software on all of your systems is up-to-date.
- Run a scan to make sure your system is not infected or acting suspiciously.
- If you find a problem, disconnect your device from the Internet and perform a full system restore.

REPORT

- File a report with the local police so there is an official record of the incident.
- Report the incident at ic3.gov.