2023/5783 High Holiday Cyber Security Checklist

**What is Cyber Security?** A set of principles and practices designed to safeguard your computing assets and online information against threats.

**Why is Cyber Security important?** Studies consistently show that 85–95% of cyber security incidents/data breaches are attributable to “end users” or human error. As individuals and organizations, we have a critical role to play in the security of our data, personal information and systems.

## Cyber Security Checklist

<table>
<thead>
<tr>
<th>Account Security</th>
<th>Organizational Cyber Hygiene</th>
</tr>
</thead>
</table>
| □ Use complex passwords for each account and ensure you do not use the same password for multiple accounts. A strong password has:  
  - Both upper- and lower-case letters  
  - Uses symbols and numbers  
  - A large number of characters—preferably 18 or more  
  - No ties to personal information such as your birthdate or the street you grew up on  
| □ Use a password manager rather than writing down passwords to help you remember them  
| □ Be wary of suspicious emails  
  - If you receive an email from an unknown person:  
    - Do not open  
    - If opened, do not open any files or click any links  
    - Report it to your IT Department, if applicable  
  - If you receive what appears to be a legitimate, but unexpected request for personal information, contact the person or the company through a verified customer service phone number to confirm  
| □ Enable multi-factor authentication on your accounts  
| □ Back up important files on either an external storage device or a secure, cloud-based platform  
| □ Encrypt your phone, computer, and external hard drives  
| □ Protect devices from malware  
| □ Password protect all devices  
| □ Ensure your devices’ operating systems and all software is up to date. When possible, enable auto update.  
| □ Avoid sending personal information over public Wi-Fi networks unless you are absolutely certain they are secure  
| □ Avoid sharing personal information on social media and check your privacy settings to ensure your accounts are not public  
| □ Keep an inventory of hardware and software on the company network  
| □ Develop a software installation process for staff and network users such as limiting installation privileges  
| □ Limit the numbers of users with administrative privileges |
Safe Surfing

☐ Check the prefix of the web address. “https” means that the website is secure whereas “http” means that it is an unsecure website. Only share data on secure websites.

☐ Check the address bar for a “locked padlock” symbol. This will also indicate that the website is secure.

Organizational Social Media Security

☐ Create a Social Media Policy
  - Create rules related to confidentiality and personal social media use
  - Identify which team members are responsible for each social media account
  - Create guidelines related to confidentiality and copyright
  - Create guidelines on how to create an effective password and how often to change passwords
  - Create guidelines for keeping software and devices updated
  - Create an action plan that identifies who to notify if a social media concern arises

☐ Train your staff on social media security issues
  - Create a system of approvals for social media posts
  - Put someone in charge of social media. The responsibilities of this person include:
    o “Owning” the organization’s social media policy
    o Monitoring your organization’s social media presence
    o Determining who has publishing access
    o Participating as a key player in development of your marketing while considering security best practices

Safe Online Video Conference Practices

- Zoom Platform
  - Consider hosting your event as a webinar, rather than traditional meeting
  - Avoid Using the Personal Meeting ID (PMI). Instead, use a new, randomly generated meeting ID.
  - Always password protect your meetings

☐ Use the waiting room function
☐ Ensure you have unchecked the box that allows participants to join before host
☐ Designate a co-host to help facilitate the meeting

• During the Meeting
  - Confirm identities of all participants prior to granting them access to the meeting
  - Limit who can share files and their screen with the meeting participants
  - Mute and/or disable the video of any disruptive participant(s)
  - Hit record during any security incidents. This could be valuable information to law enforcement partners.
  - Remove disruptive participants from the meeting

Personal Cyber Security/Digital Breadcrumbs

☐ Do not name WiFi networks after family/household names
☐ Change manufacturer or platform provided passwords after activation
☐ Log out and keep your computer locked while leaving it unattended
☐ Never insert USB flash drives/devices with unknown origins into your computer
☐ Be considerate of the information you give out online. Posting information about your current location, address or routine can leave you vulnerable.
☐ Look into the privacy settings of applications and the websites you visit to see what and how information is collected from you

Special Considerations for Kids

☐ Talk with your kids about safe online practices. You should inform your kids to:
  - Never share personal information such as your home address, school you attend or your phone number
  - Never interact with someone they do not know
  - If asked for personal information or photos, they should contact an adult immediately
☐ Kids should never download anything without an adult’s permission