Top 10 Electronic Usage Tips:

1. **Create Unique Passwords:** Use passwords that are hard to guess, unique, complicated, and long. Do not use the same password for all accounts, especially for your social media, email, and financial websites. Having separate passwords for every account helps to thwart cybercriminals. A strong password is at least 12 characters long. Focus on sentences or phrases that you like to think about and are easy to remember. Do not select "remember my password." You can utilize a password-protected password manager – from a known, trustworthy company – to securely track and store your passwords.

2. **Get Two Steps Ahead:** Turn on two-step authentication – also known as two-step verification or multi-factor authentication – on accounts where available. Two-step authentication can use anything from a text message to your phone to a biometric like your fingerprint to provide enhanced account security.

3. **Password Protect Your Devices and Electronic Data:** Engage password-protected lock screens that lock access to your devices when you are not using them and that protect your devices if lost or stolen. Do not leave confidential or sensitive documents where they can be viewed by others. Password protect confidential electronic data that you are sending to someone else. For example, if you are sending confidential data via a CD or USB drive to an opposing counsel or to an expert witness, give each individual electronic file a password for the intended person to be able to open and access the file.

4. **Keep All Machines Clean and Up to Date:** Keep the software on all devices up to date. All critical software, including computer and cell phone operating systems, security software and other frequently used programs and apps, should be running the most current versions. Utilize a spam filter in both your work and personal email accounts. Make sure all anti-virus software is up to date to detect and disable malicious programs.

5. **When In Doubt, Throw It Out:** Links in email, social media posts and online advertising are often how cybercriminals try to steal your personal information. Do not open links or attachments in an email if you do not know the source or if it looks suspicious. Even if you know the source, if something looks suspicious, delete it. Telltale signs of a phishing email include messages from companies you don't have accounts with, spelling mistakes, messages from the wrong email address, generic greetings (i.e. "Dear User," instead of your name), and unexpected messages with a sense of urgency designed to prompt you into responding quickly. If you get an email asking you for a password, or linking a page that asks you for a password, assume it is a scam. Report suspicious emails to your IT Department. Be wary of communications that implore you to act immediately, offers something that sounds too good to be true, or asks for personal information. Visit websites by typing the address into the address bar. Do not follow links embedded in unsolicited emails. Only open an email attachment if you are expecting it and know what it contains.

6. **Avoid Public Wi-Fi:** Avoid using public computers and open wireless networks, especially for sensitive online transactions. Wi-Fi spots in airports, hotels, coffee shops, and other public places can be convenient, but they are often not secure and can leave you at risk. Check whether the website you are visiting is secure. If the website you are visiting is on a secure server, it is should start with https:// ("s" for security) rather than the usual http://. If you are accessing the internet through an unsecured network, you should be aware that malicious individuals may be able to eavesdrop on your connection. This could allow them to steal your login credentials, financial information, or other sensitive information. You should consider any public Wi-Fi to be "unsecure." Do not access

sensitive accounts (i.e. banks, credit cards, etc.) over public networks. Don't walk away from your mobile device in a public space – take the device with you.

7. **Back It Up:** Protect your valuable work, music, photos and other digital information by regularly making an electronic copy and storing it safely.

8. **Plug and Scan:** USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.

9. **Delete When Done**: Many of us download apps for specific purposes or have apps that are no longer useful or interesting to us. It's a good security practice to delete all apps you no longer use.

10. **Think Before You Post:** Use discretion when posting personal information on social media, including you email address, etc. This information is a treasure-trove to scammers. Avoid posting where and when you are traveling on social media. When you reveal these specifics, you are providing information that criminals could use to target your home or your family while you are away.