State Privacy Office
December Privacy Tip

As you know, the Privacy Office occasionally issues tips for the purpose of assisting you in making informed decisions in your "away from work" life. The following tip is for that purpose (and we all know that we cannot use the internet for shopping, managing bank accounts, etc. while on the job and with State equipment!).

10 Digital Privacy Tips for the Holidays

The holiday season brings increased online activity, from shopping to travel planning. It is also a time when cybercriminals are most active. Here are ten essential digital privacy tips to keep your personal and professional information secure:

1. Shop Smart Online

Use trusted websites for holiday shopping. Look for "https://" in the web address and avoid clicking on links in unsolicited emails or advertisements.

2. Enable Two-Factor Authentication

Secure your accounts with 2FA wherever possible. This adds an extra layer of protection to your personal and work accounts by requiring a code in addition to your password.

3. Beware of Phishing Scams

Be cautious of emails, texts, or calls that ask for personal or financial information. Cybercriminals often disguise themselves as trusted retailers or delivery services during the holidays.

4. Use Secure Wi-Fi networks

Avoid public Wi-Fi for online shopping, checking work emails, or accessing sensitive information. If you must use public Wi-Fi, connect through a Virtual Private Network(VPN)

5. Keep Devices Updated

Ensure your work and personal devices are updated with the latest software and security patches. This helps protect against known vulnerabilities.

6. Protect Work Information

If you're working remotely during the holidays, use state-provided secure connections and avoid saving sensitive data on personal devices.

7. Be Cautious with Holiday Apps

Many holiday-themed apps may request unnecessary permissions. Only download apps from trusted sources, and review their privacy settings before use.

8. Secure Your Home Network

Change default passwords on your home Wi-Fi router and use a strong password to protect your network. THis is especially important if you access state systems from home.

9. Monitor Your Financial Accounts

Regularly review your bank and credit card statements for unauthorized changes. Setting up account alerts can help you quickly detect any fraudulent activity.

10. Dispose of E-Waste Securely

If you're upgrading your tech during holiday sales, remember to securely erase all data before disposing of old devices to prevent sensitive information from being recovered.

As state employees, protecting sensitive information–whether personal or related to our work–is a responsibility we share. By staying vigilant, we can enjoy a safe and secure holiday season.

Note: *Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.*

Source: Cyber Readiness Institute Staying Safe Over the Holidays