HOLIDAY CYBERSECURITY TIPS

from the Office of Internal Controls, Audit Compliance & Information Security (IAC/S)

The holidays can be a very busy time for many of us. Cyber criminals are aware of this and may attempt to take advantage of you while your guard is down.

The following safety tips will help us all to refocus for the holidays and beyond:

Protect your social media accounts

Use security and privacy options provided by social media platforms, such as a two-factor authentication system or access control. Set your accounts to private and review the default privacy settings so you can control who sees what on your accounts.

Avoid public wi-fi

Public wi-fi is one of the most common ways cyber criminals can access your personal information. When using public wi-fi, avoid those without password protection, as they are the least secure. Even if a public network in a hotel or café is protected with a password, activating a Virtual Private Network (VPN) while connecting to it is highly recommended.

Be aware of phishing scams

Phishing scams are becoming increasingly common, and they are often used to target holiday shoppers. Be aware of the signs of a phishing scam, such as unexpected emails or text messages from unknown senders.

Don’t click on links in emails

Over 15 billion spam emails are sent daily, making it easy to fall victim to phishing attacks. In 2021, more than 200,000 phishing attacks were identified, and this year, it’s expected to increase by 6 billion more.

Cyber criminals often send out fake emails or text messages with links that lead to malicious websites. Do not click on any links if you receive an email or text message from an unknown sender.

Use a credit card

When making purchases online, it’s better to use a credit card than a debit card. When you use a credit card to make a purchase, you’ll typically have some form of protection against data breaches supplied by the merchant.

Keep your software up to date

One of the best ways to protect yourself from cyber attacks is to keep your software up to date. This includes your operating system, web browser, and other software you use regularly on computers, laptops, mobile phones, and other devices.

Use strong passwords

Using strong passwords is one of the most important things you can do to protect your online accounts. Be sure to use a different password for each of your online accounts so that a hack in one doesn't affect the others.

Be careful what you share online

Cyber criminals can often gain access to your personal information by simply looking at what you have shared online. Avoid sharing personal information like date of birth, Social Security details, phone numbers, names, etc.

Office of Internal Controls, Audit Compliance & Information Security (IAC/S)
https://health.maryland.gov/iac
MDH.IAC@maryland.gov | 410-767-5314
