Check out these **Holiday Season**

Cybersecurity Tips

Auxiom
The Gold Standard in Business IT

Share these tips with your employees, friends, and family!

1 Think before you shop

Before shopping online, make sure the device you're using is up-to-date. Do your email, banking, and credit accounts have strong passwords?

Even better, if multi-factor authentication is available, are you using it?

2 If it swims like a phish...

Be cautious when clicking links or downloading files from unknown sources. Beware of emails or websites with typos or grammatical mistakes, common in phishing. Some emails can even have a link to a fake website to steal your information.

If you don't have email security software installed - now is a great time to consider it.

3 Shop where you know

When shopping online, how are you finding deals? Avoid clicking ads on web pages or links in emails and only shop through known/trusted vendors.

Remember - if it looks suspicious, something's probably not right!

4 Get only what you paid for

If you shop online often, make it a habit to check invoices, receipts, credit card, and bank statements for errors or fraudulent charges.

If you see something that doesn't look right, immediately notify your bank or financial institution and local law enforcement.

5 Back-up before you pack-up

Leaving for vacation or holiday? Closing down your offices for a week? Make sure you have proper backups for critical resources and data before you go.

Disasters can strike at any time in many forms. Proper backups can save you time, money, & your sanity!

6 Pay smarter

When paying online, use a credit card or a third-party payment system rather than a debit card.

PayPal and Venmo are better than debit cards because the store never directly receives your financial information. If your information or payment method becomes compromised, they can often offer further protection against fraud.

7 Just say "No" to public Wi-Fi

Free Wi-Fi might seem like a sweet treat, but it's risky. Don't shop on public Wi-Fi. It's usually unsecured, has no password, and anybody can connect to it.

Using your devices on public Wi-Fi to do your holiday shopping can expose your information to cybercriminals. This is especially risky if you use one device for both personal and business.

8 Work on work devices, shop on home devices

With remote working, you might be tempted to just hop on your work computer and do a little holiday shopping, but it's not a good idea.

An attacker has much to gain by getting into your employers' systems or network and you could be compromising them by using work devices for personal activities.

9 Don't just give it away

If you're going to make a purchase online, think about what information you are handing over?

Before providing personal or financial information, check the privacy policy. Make sure you understand how your information will be stored and used.

10 Use strong passwords

Using strong passwords is the EASIEST thing you can do this holiday season to safeguard yourself. The stronger and more diverse your passwords are, the better.

Even better, use a password manager! You could even gift a subscription to ensure the people you love are safer from cyberattacks!

Auxiom
805 Oakwood Dr., Suite 150
Rochester, MI 48307

info@auxiom.com
800.837.GOLD
www.auxiom.com