KEEP SAFE THIS BLACK FRIDAY AND CYBER MONDAY



Use Secure Online Shopping Websites: Before you purchase anything online, hover the cursor over the URL and confirm the authenticity of the web address. Look for the padlock symbol in the address bar and ensure that the URL begins with 'HTTPS://' rather than 'HTTP://.' The 'S' indicates that the webpage has been encrypted and secured with an SSL certificate.

Avoid Pop-up Ads: Pop-up advertisements are a common method used for spreading viruses. Clicking on these malicious ads could link you straight to a scam website or result in viruses being installed on your device.

Be Vigilant for Phishing Emails: Cyber criminals send phishing emails to trick online shoppers into clicking a link under the pretence that it is from a legitimate retailer. Avoid clicking links in emails, SMSes, or any social media platform. Instead, shop directly from the retailer's website.

Remember the Basics: Avoid doing online shopping or any other sensitive transactions over public Wi-Fi connections at airports and coffee shops. Always use a strong password and enable MFA wherever it is supported. Keep all software updated, and remember, if it is too good to be true, it is probably a scam.

Beware of Social Media Scams: Social media scams are prevalent in weeks leading up to Black Friday and Cyber Monday. Cyber criminals use social media platforms, including Facebook, Instagram, and Twitter, to put malicious posts and adverts out. The objective is to entice online customers to like and share their posts. The links are often to fake websites that either install viruses or steal payment information.

Beware of Fake Websites: Fake websites is a popular method used by cybercriminals to deceive online consumers leading up to Black Friday and Cyber Monday. They will clone legitimate websites with the objective of stealing your payment information. Look out for misspelled links and pixelated images. Always hover the cursor over links to validate the real destination URL before clicking on any link.

When Possible, use a Credit Card: It is always recommended to use credit cards instead of debit cards for online shopping. Major credit card companies, including Mastercard, American Express, and Visa, provide Zero Fraud Liability policies, so you do not need to pay for any fraud. If cyber criminals gain access to your debit card details, they can steal money from your account, and it is significantly more challenging to recover the stolen funds.

GRANT HUGHES
SPEAKER - AUTHOR - ADVISOR

CyberAwareness
Influencing change, one message at a time