How to protect yourself from cyber-scammers over the festive period

December 11 2023, by Rachael Medhurst

Credit: Pixabay/CC0 Public Domain

The festive season is a time for joy, family and festive cheer. However, it's also a prime target for cybercriminals. As online shopping ramps up, so does the risk of falling prey to cyber-attacks. That's why it's crucial to be extra vigilant about your cybersecurity during this time.

Here are some essential tips to safeguard yourself and your data during the festive period:

Phishing

Phishing is when criminals use scam emails, text messages or phone calls to trick their victims. Their goal is often to make you visit a certain website, which may download a virus on to your computer, or steal bank details or other personal data.

This type of scam tends to increase at this time due to the amount of people having bought or received new gadgets and technology.

Look out for there being no direct reference to your name in any communications, with wording such as "Dear Sir/Madam" or other terms such as "valued customer" being used instead. Grammar and spelling mistakes are also often present.

Be wary of any suspicious links or attachments within emails too, and don't click them. It's better to contact the company directly to check if the message is genuine. You can also report suspicious messages and phishing scams to the government's National Cyber Security Center.

Shopping safely online

The convenience of online shopping is undeniable, especially during the festive season. However, it's crucial to prioritize your security when buying online.

Before entering your personal and financial information on any website, ensure it's legitimate and secure. Look for the "https" in the address bar and a padlock icon, which indicates a secure and encrypted connection.

When creating passwords for online shopping accounts, use strong, unique combinations of letters, numbers and symbols. Avoid using the same password for multiple accounts, as a breach on one site could compromise all your others.

As with shopping in the real world, be cautious when encountering offers that are significantly below usual prices or which make extravagant promises. Always conduct thorough research on the seller and product before making a purchase. If a deal seems too good to be true, it probably is.

And if you are out shopping in towns or city centers, there will often be a large number of public wifi options available to you. However, criminals can intercept the data that is transferred across such open and unsecured wifi. So, avoid using public wifi where possible, especially when conducting any financial transactions.

Social media

While social media platforms provide people with a means to keep in touch with family and friends over the festive period, they are often a goldmine for scams and malware (software designed to disrupt, damage or gain unauthorized access to a computer). In the spirit of the festive season, people often share an abundance of personal information on social media, often without considering the potential consequences.

This trove of data can make people vulnerable to cyber-attacks. Scammers can exploit this information to gain unauthorized access to social media accounts, steal personal information, or even commit identity theft. To protect yourself, be mindful of what you share.

Be wary when interacting with posts and direct messages, especially if they contain suspicious links or attachments. Before clicking on

anything, hover over the link to verify its destination. If it shows a website you don't recognize or seems unrelated to the message, do not click on it. If you receive a message from someone you know but the content seems strange or out of character, contact them directly through a trusted channel to verify its authenticity.

Likewise, be wary of messages containing urgent requests for money or personal information from businesses. Genuine organizations will never solicit sensitive details through social media.

There are many buy and sell platforms available on social media. But while such platforms can be a great place to find a unique gift, it is also important to remember that not all sellers may be legitimate. So, it's vital that you don't share your bank details. If the seller sends a link to purchase the item, do not use it. When meeting to collect an item, it's generally safer to use cash rather than transferring funds electronically.

Package delivery scams

As well as being a time for giving and receiving gifts, the festive season is also ripe for cybercriminals to exploit the excitement surrounding package deliveries.

Scammers often pose as legitimate delivery companies, sending emails or text messages claiming that a delivery attempt was unsuccessful or requiring additional fees for processing, or even customs clearance. Typically, these messages contain links or phone numbers that, when clicked or called, lead to fake websites or automated phone systems designed to collect personal information or payments.

To protect yourself, always verify the legitimacy of any delivery notifications you receive. Check the sender's email address or phone number against the official contact information for the delivery

company. If the information doesn't match or seems suspicious, don't click any links or provide personal details.

Legitimate delivery companies will never ask for upfront payment or sensitive information through unsolicited messages or calls.

Remember, cybercriminals are skilled at manipulating the festive spirit to their advantage. Stay vigilant, exercise caution, and don't let your excitement for gifts and deliveries compromise your cybersecurity.

Provided by The Conversation