Security Hints & Tips: Holiday Shopping

For many of us, the holiday season is about friends, family, food, and shopping! Two of the busiest shopping days of the year, Black Friday and Cyber Monday, are at the end of November. Unfortunately, while you're looking for the perfect gift, cybercriminals are looking for ways to scam you. Follow the tips below to shop safely:

Never install unfamiliar software.

There are hundreds of shopping apps out there. Some of these apps may be malicious, so only use apps that you know and trust. When you download software or apps, be sure to download from verified sources such as the App Store or Google Play. You can verify that an app is legitimate by reading the app's reviews, checking the number of app downloads, and looking up the app's developer.

Verify attachments are safe before downloading them.

A common tactic among cybercriminals is to create phony email notifications from a retailer or postal service. These notifications often include a malicious attachment. The cybercriminals may claim that there was an update to your order or that your package has been delayed, but you'll have to download the attachment to find out more. Don't fall for this trick! Before you open the attachment, contact the retailer or postal service to verify that the notification is legitimate. You can also look up your order directly on the website where you made the purchase.

Verify links before clicking.

Watch out for malicious advertisements, otherwise known as malvertising. Malvertising is when cybercriminals use ads to spread malware or to trick users into providing sensitive information. When online shopping, only click on an ad or link from a reputable source, such as a retailer's official social media profile. To be extra careful, use your browser to navigate to the store's official website to shop instead.

The KnowBe4 Security Team
KnowBe4.com