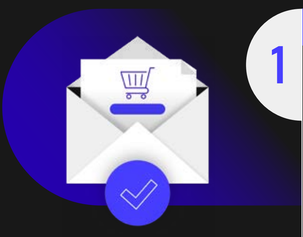
Secureworks

2024 CYBERSECURITY TIPS FOR BLACK FRIDAY & CYBER MONDAY

Black Friday and Cyber Monday can expose online shoppers to increased risk of cybercrime. This year, adversaries may exploit issues affecting global supply chains by playing on themes around inflation, rising energy prices, shortages of goods and increased delivery timescales.



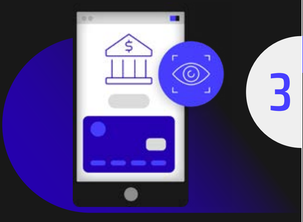
1 VERIFY EMAIL SENDER

Check the sender address for any email that invites you to scan a code, click a link or open an attachment. Look for misspellings of domain names or discrepancies between the display name and the actual sender email address. **Be especially wary of emails from retailers you do not recognize or have not previously used.**

SKIP THE SCAN

Some deals can be too good to be true. **Beware of lookalike sites that offer deep discounts and hard-to-find products**. Even if a website or email looks legit, open a new browser whenever possible to visit the real eCommerce site directly rather than scanning a QR code or clicking on links through an email.

2



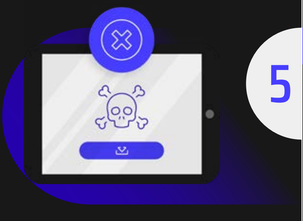
3 WATCH YOUR BANK ACCOUNTS

Sign up for fraud alert notifications from your bank or card provider. This safeguards you against scams that falsely claim there has been unauthorized activity on your accounts in order to trick you into divulging your account login and password.

ADD SECURITY TO YOUR STORE ACCOUNTS

Use multi-factor authentication on all accounts that will allow it and a strong, unique password for every site. If your credentials are stolen, this can significantly reduce the chances of cybercriminals being able to use them to access your personal information, bank details or to conduct fraudulent transactions.

4



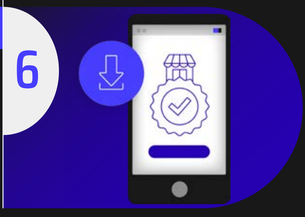
5 DOWNLOAD CAUTIOUSLY

Malware infections can occur via malicious advertising ('malvertising') or third-party code running on e-commerce sites, so visitors get infected through no fault of their own. **Never let a website bully you into running downloaded software or call a tech support hotline.**

CONTROL APP PERMISSIONS

Only download mobile apps from authorized app stores, not via QR codes you aren't sure of. Even then, be aware of what permissions they are asking for. Apps that ask to access your text messages, contact lists, or passwords should be treated as highly suspicious. Remove any apps that you don't need or don't use any more.

6



Whether it is preying on holiday shoppers or your organization's employees, adversaries are continually looking for ways to exploit gaps and errors to maximize the payoff of every breach.

READ THE 2024 STATE OF THE THREAT REPORT →

Secureworks