

CybeReady Releases Five Easy Tips to Shop Safely During Black Friday

Safe Shopping Guidance Coupled with New CISO Tool to Help Safeguard Personal Data and Corporate Networks



CybeReady

SANTA CLARA, CALIFORNIA, UNITED STATES, November 21, 2022

/EINPresswire.com/ -- [CybeReady](#), provider of the world's fastest security awareness solution, today announced five easy security tips to help holiday shoppers safely navigate Black Friday and Cyber Monday as holiday sales put employee data and corporate networks at risk. Coinciding with Black Friday, the company is also releasing its enhanced [CISO Toolkit](#) to provide complimentary tools with guidance on safe online shopping to help CISOs defend employee desktops, laptops, mobile devices, and connected corporate networks.

According to the [FBI](#), "Every year, thousands of people become victims of holiday scams. Scammers can rob you of hard-earned money, personal information, and, at the very least, a festive mood."

Shopping scams are notoriously active during Black Friday and Cyber Monday as millions of shoppers use their PC, laptop, or mobile device to scan for deals and make purchases. This presents a considerable risk to organizations with a large number of employees working remotely. These scams often focus on obtaining the victim's financial information with methods that include phishing scams, advertising lures, push notification lures, and payment traps.

Black Friday and Cyber Monday phishing emails tend to showcase amazing deals. Oftentimes these offers use emotional tactics to lure consumers into clicking offers that don't really exist. Consumers expect deals, so phishing emails on Black Friday focus on deals more than any other type of scam. Advertising lures entice the user to enter a fake website and provide credit card information. Payment traps force the user to submit their credit card information rather than using a digital wallet or payment service, allowing the capture of this sensitive payment information. Other factors weaken the buyer's judgment, making the situation even more dangerous as limited-time deals make it difficult to dig into the details, and unknown senders frequently text and email the buyer, adding to the distraction.

So, when this unique shopping season arrives, it is critical to be hyper-aware of the increasing risks to personal finances and employer networks. In response, CybeReady is offering the following guidelines to help reduce the chance of a scam or other sinister attack achieving success:

Before Shopping:

1. Always enter the URL for a merchant's website yourself. Do not use a link from an ad or email. Use the brand's official shopping application on your smartphone.

While Shopping:

2. Check for the lock symbol next to a website's URL to ensure it is a secure site.
3. Use a third-party payment method that does not transmit credit card information to the seller (like PayPal or Venmo), or use a disposable card.

After Shopping:

4. Visit the merchant's website to see sales updates. Do not click links in emails or texts claiming to provide order updates.
5. Keep an eye on your financial account for any unanticipated transactions.

Because some employees will inevitably use their corporate connected PCs, laptops and mobile devices to take advantage of short-term shopping specials, CISOs are also advised to implement additional safeguards during this time period. To assist security leaders, CybeReady is releasing its enhanced CISO Toolkit for the holidays, which provides complimentary tools to help communicate relevant security information to employees – quickly and effectively. Download the free CISO Toolkit [here](#).

The enhanced toolkit provides an overview of security guidelines, policies and tips, offering easy-to-understand information to help avoid cybersecurity traps with guidance on:

1. Holiday Shopping Security
2. Zoom Security
3. Online Privacy
4. Password Security
5. Fake News and Rumors
6. Remote Work
7. COVID-19-related Phishing Emails
8. Security in Times of Crisis
9. Sextortion - what employees need to know
10. Tips for Worry-Free Vacations

"It is important to realize how good deals for employees can become a bad ordeal for your organization," said CyberReady CEO, Eitan Fogel. "During the Holiday Season employees may be easily distracted and hackers are very aware of this, resulting in a significant increase in cyberattacks as the holidays approach. In response, it must be an all-hands effort to ensure security is a top priority."

Tweet This: [@CybeReady Releases Five Easy Tips to Shop Safely During Black Friday](#)

- <https://cybeready.com/category/news>

Resources:

- CybeReady Case Studies - <https://cybeready.com/resource-center/case-studies>
- CybeReady White Papers - <https://cybeready.com/resource-center/white-papers>
- The Ultimate Guide of Security Awareness Training - <https://cybeready.com/complete-guide-cyber-awareness>

About CybeReady

CybeReady offers the world's fastest security training platform, that evolves your organization from security awareness to cyber readiness. CybeReady's solution autonomously engages more employees, more effectively, frequently, and easily. Infused with training expertise and powered by machine learning, CybeReady's adaptive, easy-to-digest security training content program guarantees to reduce your high-risk employee group by 80%. CybeReady's fully-managed solution has been deployed by hundreds of enterprises worldwide, including the City & County of San Francisco, SodaStream, ING, StitchFix, Teva Pharmaceuticals, Avid Technology, and others, CybeReady is fully-managed, making it the security awareness training solution with the lowest total cost of ownership (TCO) available today. Founded in 2015, CybeReady is headquartered in Tel Aviv, Israel, with offices in the Silicon Valley. For more information, please visit www.cybeready.com.

- END -

Joe Austin

Media

+1 818-332-6166

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/602410907>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2022 Newsmatics Inc. All Right Reserved.