Stay Safe This Amazon Prime Day: Keeper Security's Expert Tips to Navigate Cyber Threats

Amazon Prime Day, one of the year's busiest online shopping events, is also a prime target for cyber attacks. Keeper Security provides essential best practices

LONDON, UNITED KINGDOM, July 15, 2024 /EINPresswire.com/ -- As Amazon Prime Day approaches on July 16-17, online shoppers are gearing up for a slew of deals and discounts. However, the increased traffic and excitement around this global retail event also attract cybercriminals looking to take advantage of unsuspecting shoppers. It is crucial for consumers to remain vigilant to protect their credit card numbers, accounts and personal information. Keeper Security, the leading provider of zero-trust and zero-knowledge cybersecurity software protecting passwords, passkeys, privileged access, secrets and remote connections, shares essential best practices to help mitigate threats and shop safely.

> As the excitement of Amazon Prime Day builds, it's important to remember that cybercriminals are just as eager to take advantage of this event as shoppers are to find great deals."
>
> *Darren Guccione, CEO and Co-founder, Keeper Security*

Cybercriminals are constantly developing new, sophisticated methods to execute their attacks. During Prime Day, fake Amazon notifications and deals are rampant, threatening the data security of unsuspecting shoppers. Phishing attacks, ransomware, malware, email compromises and falsified QR codes are all common tactics used to deceive consumers into falling for scams. To counter these threats, shoppers should adhere to the following best practices:

Shop on the Official App or Website: Scammers often create fake websites that mimic those of well-known companies to lure in unsuspecting customers. To avoid falling victim to these schemes, always shop directly through Amazon's official app or website. Avoid entering the site from third-party messages or links, as these could be scams. Additionally, keep an eye out for false advertisements in search results that could lead you to a spoofed version of the legitimate website. For example, the URL www.Amazon.com could be changed slightly to www.Amaz0n.com

on a dangerous, phoney website.

Beware of Phishing Scams: With millions of users searching for the best Prime Day deals, cybercriminals may send emails or text messages urging shoppers to click on links or provide personal information. These links often lead to fraudulent websites that mimic legitimate retailers and entice consumers with unbelievable deals or prices. Shoppers may be prompted to fill in their credit card or account information on these fake sites, giving cybercriminals access to their sensitive data. Always check the sender of an unsolicited email, check URLs before visiting a website and don't open any attachments you weren't expecting – especially from unverified senders. Be cautious of messages with typos, too-good-to-be-true offers or requests to click links immediately, as these are common indicators of scams.

Use a Strong and Unique Passwords: All of your accounts should be protected with strong passwords. A strong password is at least 16 characters and uses uppercase and lowercase letters, along with numbers and symbols. Passwords should be unique for every account, because if a cybercriminal gets a hold of a password that is reused across multiple accounts, the bad actor can access all of them. A password generator can generate strong passwords for all of your accounts. Better yet, a password manager can generate, store and automatically fill the passwords for all of your accounts, while also providing a built-in warning about spoofed websites.

Enable Multi-Factor Authentication (MFA): MFA adds one more layer of security by requiring multiple verification methods before granting access to an account. This additional security step helps ensure that even if a password is compromised, cybercriminals will still be thwarted when trying to enter the account. Enabling MFA is a critical step in fortifying your defences. A secure password manager can not only generate and store strong passwords, but also store and automatically fill your MFA codes.

"As the excitement of Amazon Prime Day builds, it's important to remember that cybercriminals are just as eager to take advantage of this event as shoppers are to find great deals," said Darren Guccione, CEO and Co-founder, Keeper Security. "At Keeper, our goal is to equip our users with the knowledge and tools necessary to defend their personal information from increasingly sophisticated cyber threats. Remember, cybersecurity isn't just about technology – it's about being aware and proactive in safeguarding your personal information."

Staying informed about the latest cybersecurity practices is essential to protect yourself online, especially during high risk events such as Amazon Prime Day. Understanding the importance of only visiting legitimate websites, watching out for phishing scams, following strong password practices and enabling MFA, can significantly enhance your security. It is better to be sceptical, as cybercriminals thrive on exploiting weaknesses.

By following these steps, shoppers can enjoy the discounts and excitement of Amazon Prime Day while ensuring their data remains secure. Don't let cybercriminals turn a great deal into a

costly scam.

Bethany Smith
Eskenzi PR
email us here
Visit us on social media:
Facebook
X
LinkedIn
Instagram
YouTube
TikTok
