BIZCOMMUNITY

6 ways to safeguard yourself this Black Friday, Cyber Monday

By Nithen Naidoo

17 Nov 2020

Black Friday is fast-approaching, and as you start planning your shopping sprees on online stores, it is imperative to ensure your personal data is secure.

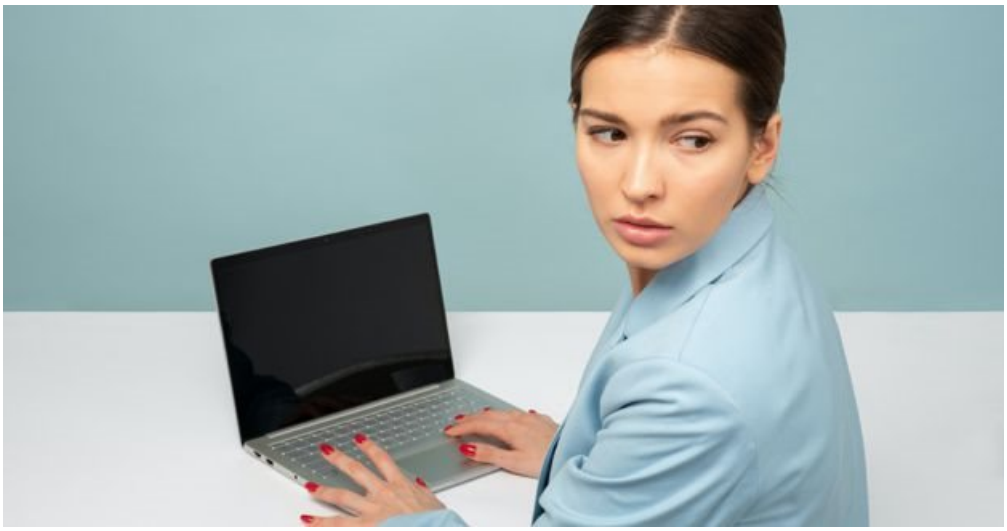

Photo by Icons8 Team on Unsplash

With the Covid-19 pandemic still in effect, more retailers are moving from brick-and-mortar to online trade; as such, Black Friday weekend is one of the biggest digital transaction hotspots on the calendar and opens us up to a multitude of cyber risks from potential criminals, such as malware, phishing schemes and data hacks.

Here are six ways to ensure that your online time is safe during Black Friday weekend:

1. **Lookout for HTTPS** - When shopping online, check that the URL begins with HTTPS, not just HTTP, or has a little lock icon next to it. This means that the site has security measures in place, ensuring that your browsing is encrypted and safe.
2. **Avoid saving financial info on shopping sites** - Websites with SSL verifications can still be hacked. Online stores allow you to save your card information on your profile for future purchases, but if you can access this information, chances are that hackers can, too. It's better to secure your financial details by removing it completely after purchasing.
3. **Use reputable sites only** - When doing your Black Friday shopping, the safest bet is to stick with well-known online retailers with established payment gateways such as PayPal and card payments.

   Some sites might look legitimate, but could redirect you to a malicious payment gateway - always use reputable payment gateways with the necessary verification and security methods in place. Retailers requesting wire transfers is an immediate no-no.

A shift in strategy on the cards for Black Friday 2020

Michael Smollan 12 Nov 2020

4. **Create strong passwords and change them often** - People often use the same simple passwords across applications, which puts your accounts at risk of malicious password-breaking malware. Never use the same online password: if one site gets hacked, your credentials can be used to access other sites.

   When devising a password, aim for something that is at least 12 characters long; a whole sentence or catchphrase is often more complex than a single word combined with numbers and symbols. A key vault can be used to store these passwords and even generate strong passwords.

5. **Enable two-factor authentication when signing in** - Multi-factor authentication - or login approval - is a series of verification steps that create an additional measure of security over and above your username and password.

   When logging in, this security measure prompts you to have to identify yourself again - often with a one-time code sent to another device or platform, and more recently through biometric verifications such as fingerprint scans or facial recognition.

   Look out for two-factor authentication on shopping sites, and ensure this is enabled from your banking service provider.

6. **Be wary of sharing your information for marketing purposes** - When completing a transaction online, users are often prompted to avail their personal information, such as names and contact details, for marketing purposes - this could be abused and can be in contravention of the pending PoPia legislation due in June of next year.

   Also never provide personal information over the phone - no retailer, courier or bank will ever ask for your credit card details, pins or verification codes when shopping online.

ABOUT THE AUTHOR

Nithen is the CEO and founder of Snode Technologies.