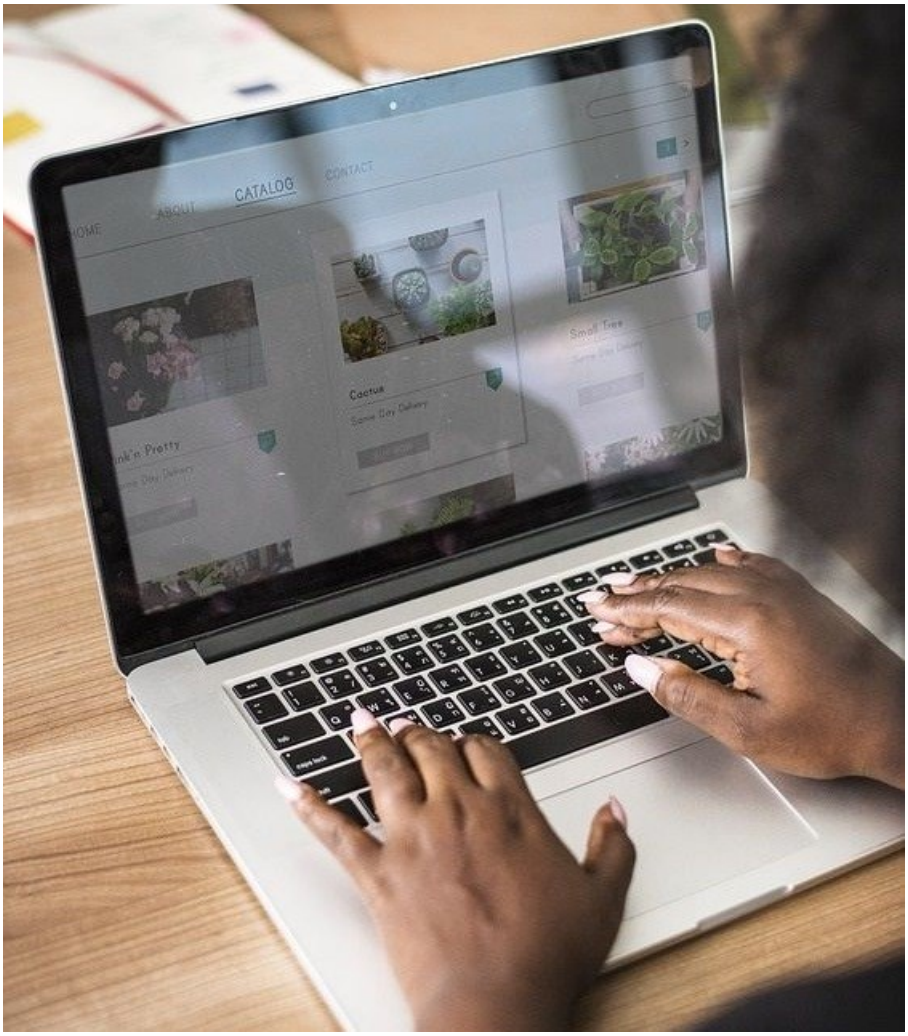
Protect yourself when shopping online

Here are tips and advice on what to do before, during and after your Black Friday online shopping sprees, to protect yourself from possible hackers and identity theft.



Source: pixabay.com

Cyberattacks, data breaches and hackers are a constant threat in today's digital world. ThisIsMe deals with identity verification for some of the largest companies in South Africa and have first hand experience dealing with fraud and protecting individuals private information online.

The problem is, once your information is in the hands of any “trusted” organisation, including banks, social sites and online retailers (e-commerce sites), it really is out of your control and you are at the mercy of often outdated IT systems and well-equipped hackers.

Events like Black Friday are a potential gold mine for hackers and scammers as millions of people flock to online retailers like Takealot to get the best deals and without hesitation will enter their confidential, personal information into any site with another "unbeatable" deal.

With this in mind and the fact that no-one wants to miss out on any Black Friday deals, here are some top tips and advice on how to protect yourself and your family when transacting online.

American Express top tips for Black Friday

OnPoint PR 16 Nov 2018

These tips are basic guidelines, taking into consideration that some of your information has already been breached (even if you don't know about it) and how to protect yourself from further damage.

Protect yourself

1. Check if you are at risk

A recent study sponsored by IBM found that on average it took 150 days for a data breach to be discovered in South Africa. Make sure you are regularly using a breach checker to monitor recent breaches and investigate if you have been compromised. Don’t wait to be notified of a breach because as the study shows, by the time the breach is detected, it’s too late.

2. Set up alerts

The next step in preparation is to set up alerts that notify you when there is a breach when your information is compromised and if there is potentially suspicious activity on your accounts or profiles.

Alerts like these will ensure that you are aware when a breach has occurred and will monitor your profiles to ensure you are not the potential victim of identity fraud as a result.

Sites like Facebook, Twitter and your bank should notify you of any suspicious activity, so do a little bit of research and make sure these notifications are set up. You can also sign up to a site like Have I Been Pwned, to get notified about any breaches that have happened and if your information is found in a breach.

3. Cover the essentials

These points have been spoken about endlessly but it’s amazing to see that most people still don’t abide by them. If everyone followed these basic steps, we would see a lot fewer cases of identity fraud and theft.

- **Password management** - The easiest way to ensure all your passwords are secure and strong, is to use a password manager such as LastPass. If you haven't already, you need to stop using the same password or similar variations for all your accounts.

- **Set up 2-factor authentication** - This simple step will add an extra layer of security to any account or profile. It helps to ensure that any hacker can't gain access to your accounts with just a leaked password.

- **Anti-Virus** - Make sure you have strong and effective antivirus software installed for all your devices, including your web browser, period.

- **Activity in public domains** - Try to avoid using public and unsecure Wi-Fi networks wherever possible. Avoid filling in any sensitive information and don't save any of your credentials, such as passwords and credit card info. You should also clear your browser cookies and cache regularly as hackers can, and will, use this information.

- **Contacting the relevant institutions** - In the event any of your information is breached or there is any suspicious activity on your profiles, contact all relevant institutions immediately, such as your bank, credit providers or insurers.

Safeguard your customer relationships this Black Friday

Wynand Smit 13 Nov 2018

4. Educate yourself on social media

These days almost everyone has a social account, which is great for sharing where you went on holiday or what you had for breakfast but not so great for protecting your personal information. Revealing your personal information is great for hackers and cybercriminals, who can use this to help answer security questions, commit identity fraud or steal your identity altogether. The worst part is you not only have to worry about criminals but the organisations themselves, who regularly share your data with third parties.

Educate yourself on what each site's security settings are, what the privacy policy covers and understand exactly who can see your information, who has access to it and who can share it. You will probably be shocked to see how little privacy and control you have over your own data.

5. Be aware of common cyber attacks and fraud scams

The most common forms of fraud and cyber attacks are phishing scams and socially engineered malware.

Both types are similar, in that they aim to defraud an individual via the use of websites, email, phone or some other form of online communication for their own gain. Phishing attempts to gather sensitive information from individuals and Malware attempts to infiltrate your system by downloading some form of malicious software.

There is little you can do to prevent attempted attacks such as these but simply being aware of the threat, means you can stay alert and will have an advantage over those who are unsuspecting and oblivious.

Final thoughts

Beyond tips and guidelines, the best thing for anyone to do is simply be aware of what is happening around them (in the real world and online), look out for any suspicious behaviour, be vigilant of what information you share, who you are interacting with and never accept anything at face value.

Don't let this deter you from getting the deal you've been waiting for all year, just don't get distracted by all the hype.