Retailers and shoppers are gearing up for one of the busiest shopping weekends of the year, but unfortunately, they're not the only ones.

This hive of online spending attracts the attention of cybercriminals who are keen to take advantage of this mass market to launch their online scams.

Black Friday is a significant shopping event that originated in the United States but has grown in popularity. It falls on November 27th this year and marks the start of a shopping bonanza when retailers sell off their stock at discount prices.

Cyber Monday follows, and it's become an even more significant event as shoppers go online to avoid the frenzied crowds that hit the shops on Black Friday. Cybercriminals follow the money, and this weekend of crazed spending provides them with the perfect opportunity to scam many people. With attacks becoming more sophisticated, shoppers need to be extra cautious when looking for the latest bargains online. Here are 10 Cyber Safety tips to keep you safe online this Black Friday and Cyber Monday using your home computers..

1. Watch out for fake websites

This is one of the most popular ways criminals will try to trick shoppers into falling for their Black Friday and Cyber Monday scams. The fraudsters will clone websites to dupe consumers into thinking they are shopping on a legitimate site. The website may appear almost identical to the real site; however, subtle changes can indicate that all is not as it seems.

A web address that ends in.co.uk may be changed to a .org, images may be pixilated, functions on the site may not work properly and the content will often be sub-standard. It's always worth double- checking the address of a site to confirm its authenticity.

2. Only use secure sites

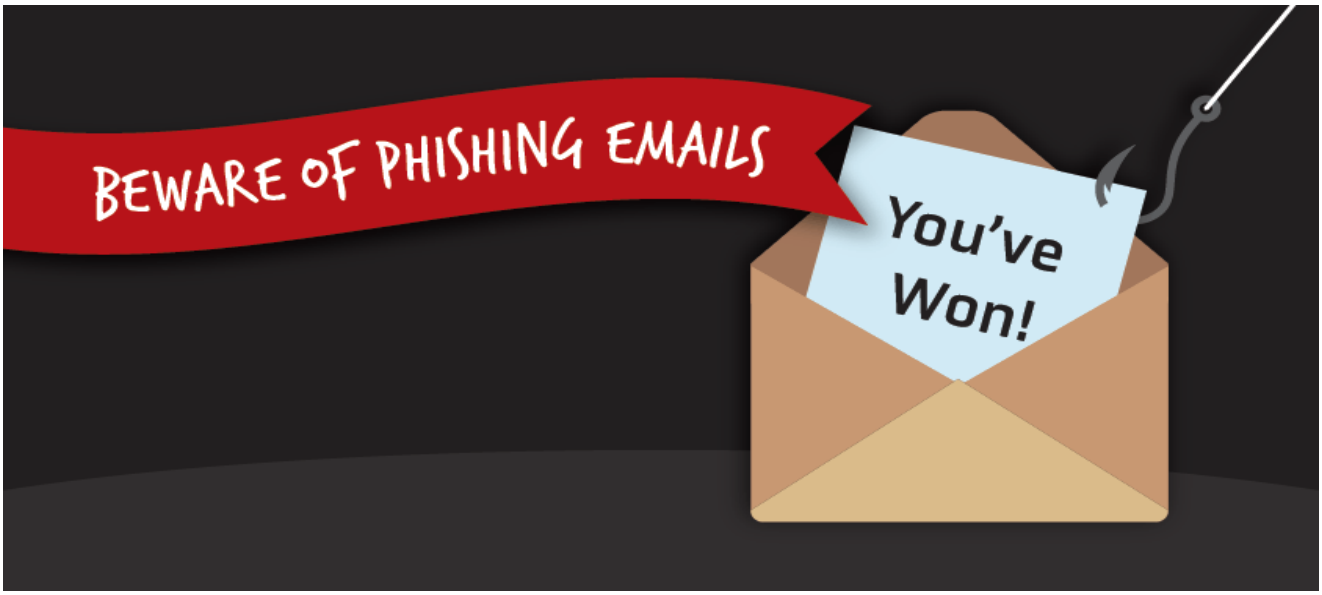
Before entering any information into a website on Black Friday, you should always check that the site is safe and secure. The first step is to hover your mouse over the URL and check the validity of the web address. You should look for a padlock symbol in the address bar and check that the URL begins with a 'https://' or 'shttp://'. The 'S' indicates the web address has been encrypted and secured with an SSL certificate. Without HTTPS, any data passed on the site is insecure and could be intercepted by criminal third parties.

However, this system is not totally fool proof. Within the last year, there has been a notable increase in the number of phishing sites using SSL certificates. Users are advised to be extra cautious and look for further evidence that the site is secure.

3. Use a credit card for shopping online

When possible, it's always best to use a credit card when shopping online as it offers additional protection over other forms of payment. If a fraudulent purchase is made on your credit card, there's a good chance your bank will reimburse you straight away. However, if a criminal steals your debit card details, they can clear out your personal account and it can be more difficult to claim the money back.

4. Beware of phishing emails



Phishing is one of the most popular ways for criminals to steal your personal information and there is always a massive increase in these types of scams on Black Friday and Cyber Monday. The speed, convenience and high return on investment makes phishing one of the easiest ways for cybercriminals to steal your personal data without you even knowing.

As Cyber Monday approaches, be wary of any emails offering cash prizes or last-minute deals. These emails are designed to trick shoppers into clicking on a link which may appear to come from a well-known retailer. Trust your gut if you think there's something not right about the email and delete it immediately.

5. Avoid deals that are too good to be true

Black Friday and Cyber Monday feature lots of legitimate deals offered by trusted and reputable retailers. However, cybercriminals know we'll be scouring the web for the cheapest deals and they take advantage of this by slipping in lots of fake offers.

Be wary of any emails, pop-ups or posts on social media promising rock bottom prices. Clicking on the link could bring you straight to a phishing site or you may end up downloading malware onto your device. It can be hard to distinguish between a real bargain and a fake so it's best to do your research to find out if the site is credible or go directly to a brands website to determine if the deal is real. It's always worth remembering that if an offer seems too good to be true, it usually is!

6. Use strong passwords

You'll have heard it us a million times, but creating a strong password really is one of the easiest ways you can protect yourself from being hacked online. With so many passwords to remember, it can be tempting to use the same password for multiple accounts, however, this puts you at great risk of having your data stolen. If hackers can work out just one of your passwords, whether it's a Facebook account or online banking details, they can potentially access every single account you have.

It's always best to use a unique username and password for separate online accounts so that in the unfortunate event of being phished, the attackers won't have access to your other online accounts. Your password should also be strong and difficult to crack. It's best to create a password that is between 15-20 characters long, contains a mix of upper and lowercase letters, and include numbers or symbols.

7. Watch out for social media scams

Social media scams are rife on Black Friday and Cyber Monday. The crooks know that people are going online to specifically look for deals, so they make it as easy as they can for shoppers to fall for their online scams. Facebook and Twitter tend to be the favoured choice for these malicious posts and criminals will ask shoppers to like and share their posts, so they're boosted to the top of news feeds and reach a wider audience.

In recent years, cybercriminals have turned their attention to social media as it provides the ideal place to dupe people into clicking on dodgy links. Users tend to be more trusting on social media and it's more difficult to determine if a link is malicious than it would be on a more traditional platform.

8. Avoid Public Wi-Fi to go shopping

Using public Wi-Fi to search for the best Black Friday and Cyber Monday deals could open you up to a range of security risks.

Public Wi-Fi requires no authentication to establish a network connection, allowing fraudsters direct access to any unsecured devices on the same open network. This enables hackers to steal valuable information such as login passwords, credit card info and other personal and financial details.

Unsecured Wi-Fi networks can also be used to spread malware allowing criminals unrestricted access to everything on your device. This information can in turn be used to commit identity fraud, or the information can be sold on to criminal third parties.

9. Ensure all your software is up to date

Before going online to shop about for the hottest deals, you should make sure that all your security software is up to date. This will prevent cybercriminals from gaining access to your computer through vulnerabilities in older and outdated systems. The installation of anti-virus software will also help detect threats on your computer and block unauthorised users from gaining access.

10. Monitor bank statements for fraudulent activity

It's always worth keeping a close eye on bank statements to make sure there are no unusual transactions on your account. Criminals know that during Black Friday and Cyber Monday there will be lots of online activity, so they hope that any unusual debits from your account will go undetected. Typically, the crooks will make a few initial debits for smaller amounts then go in for a larger amount which could clean out your bank account.

Despite the increasing sophistication of phishing attacks there are a number of ways you can protect yourself online. MetaPhish has been specifically designed to protect businesses from phishing and ransomware attacks and provides the first line of defense in combating cyber-crime. Get in touch for further information on how we can help protect your business.