BIZCOMMUNITY

Safe shopping starts with awareness

By Brian Pinnock

22 Nov 2018

One of the most common pieces of advice we get about avoiding phishing scams is that, if it seems too good to be true, it probably is. Except this doesn't really apply on Black Friday.

Source: pixabay.com

For one day a year, on 23 November this year, retailers take advantage of consumers' appetite to spend by offering "loss leader" deals, which they advertise broadly on email and social media.

The purpose of these offers is to entice shoppers to retailers' sites and stores and convince them to buy more than the too-good-to-be-true TV for R500. And cybercriminals know and take advantage of this.

There's good news and bad news for Black Friday shoppers this year. The bad news is that cybercriminals are using new tactics that make it harder to spot fake deals. The good news is that with robust cybersecurity awareness training, an understanding of the new attack methods and sophisticated email security systems, consumers can protect their money and personal information, and businesses can better protect their sensitive data and systems.

Old dogs, new tricks

Black Friday is like Christmas for hackers. While you're shopping for bargains, they're shopping for your credentials, which they use to log into your internet banking and other online accounts to steal your money.

If cybercriminals have your login details, they can access your profile even on sites implementing good security practices. Criminals are hitting various online services with credentials in the hopes of a password and username being accepted as legitimate.

#BlackFriday: Protect yourself when shopping online

19 Nov 2018

Black Friday grows every year in South Africa. Last year, sales increased by 2571% over 2016 as more retailers jumped on the bandwagon. This year will be even bigger, which means gullible and uninformed consumers – many of whom work for enterprises - are ripe for the picking. And chances are they aren't aware of the new tactics being used against them.

Forget everything you know about cyber security

Ok, maybe not everything. But a lot of what we know about cybersecurity, and the tips and tricks that protected us in the past, no longer apply to some phishing attacks.

As we've already learnt, we're often told to be suspicious of ridiculously cheap deals, but on Black Friday, ridiculously cheap is expected, so we're not likely to question R500 TVs.Another thing we're told is to look for the green or black padlock on a website, or for the all-important **'s'** in **'https'** of the site's URL. But we can't even trust this anymore. That's because cybercriminals can create or buy a real security certificate for their fake website in minutes.

One site issued over 14,000 SSL certificates to "PayPal" sites – 99% of these were used for phishing fraud. So, while a fake website looks secure, it really isn't.

So, what security advice is still valid?

- **Look out for spelling errors in emails**. While the days of phishing emails with dozens of grammatical errors are gone, many cybercriminals still deliberately include a few to filter out smart people and target those who are not paying attention
- **Don't click on links within emails**. Enter the site's address directly into your browser. If you can't find the deal that was advertised in the email, warning bells should be ringing.
- **Check the sender's address**. Takealot won't send you an email from a Gmail account, they will use their domain.
- **Be password smart**. Don't re-use passwords across multiple services
- **Use two-factor authentication (2FA) wherever possible**. This makes it harder (but not impossible) for criminals to use your username and password against you if your credentials have previously been stolen.

New and evolving attack methods

Cybercriminals increasingly use various forms of domain similarity– when they subtly change characters and words in URLs and email addresses to match a trusted organisation. These types of attacks often bypass certain email security systems because the sites and email senders aren't known to be malicious.

To create lookalike domains, attackers often use non-Western character sets to display letters that look identical to the

naked eye. Mimecast.com, for example, looks like мimecaѕт.com in Cyrillic. You might think we're getting fancy with our font. We're not. Combined with a legitimate certificate, it becomes much harder to spot a fake website.

This creates prime conditions for a successful phishing attack: nearly half of all South African firms in a recent Vanson Bourne and Mimecast research report saw an increase in targeted spear phishing attacks using malicious links over the past year.

> Quick tip: Check the URL carefully. A very long URL might be a sign that the website is fake. However, these are difficult to spot when browsing on a mobile phone, unless you scroll all the way. Rather check on your computer to be sure.

Stay safe in the wild

Consumers and businesses can stay safe this Black Friday.

> Here's how:
>
> - Be suspicious by default. Don't trust any email and go straight to the retailer's website instead of clicking on links.
> - Create a separate email address when signing up for Black Friday alerts. Don't use your work or personal email.
> - Use a separate credit card for online purchases to limit your losses if you are attacked.
>
> - Conduct regular security awareness training to ensure all employees have the awareness to spot potential cyber threats. Human beings are an organisation's greatest cyber risk and its best defence against cybercrime. During high-risk periods such as Black Friday, unaware users could expose the organisation and their families to unwanted cyber risk. Focus on implementing effective, modern training techniques and create a human firewall around sensitive company data.

The threat landscape has evolved yet again. We can never let our guard down and we have to assume that we're never completely safe – even if we have robust security systems in place. Apple CEO Tim Cook said recently that cyber resilience is like running on a treadmill. You can't just stop. If you do, you'll fall off and will probably get hurt.

via GIPHY

Stay alert. Stay safe. And happy shopping!

ABOUT BRIAN PINNOCK

Director of Sales Engineering at Mimecast
- #BizTrends2021: What the new year holds for cybersecurity - 6 Jan 2021
- #BizTrends2020: Cybersecurity trends predictions - 16 Jan 2020
- Control+Z your data - 29 Mar 2019
- #BizTrends2019: South African cybersecurity trends for 2019 - 21 Jan 2019