






BLACK FRIDAY PHISHING!








Black Friday & Cyber Monday is the time of the year that phishing grounds are the most lucrative for cybercriminals, with attacks increasing by as much as 336% around this time^[1]. This not only poses a threat to consumers but also organisations.

While retailers should go to great lengths to protect our data, as consumers, it remains our responsibility to keep our own information safe.

Some of the tactics criminals use to wreak havoc during the shopping frenzy:

-  Spoofed landing pages are a firm favorite at this time of the year
-  Cybercriminals find ways to circulate scam posts through social media platforms claiming false promises with deals like massive discounts and freebies.
-  Scam URLs - mobile users are often susceptible to this scam as they often do not check the full URL on their device. This is an easy way to trick people into thinking they are buying the real thing when they are not.

Don't get hooked

-  Verify websites, especially when directed via an email, text or online advert
-  Keep your card and its details safe
-  Use secure and trusted WiFi
-  Keep a close eye on your bank statements
-  Keep software up to date and allow for patching

[1] <https://www.information-age.com/black-friday-security-threats-123476732/>