Wait...is that the real Facebook?

Check Point Research, a provider of cybersecurity solutions globally, has published its new Brand Phishing Report for Q4 2019. The report highlights the brands which were most frequently imitated by criminals in their attempts to steal individuals' personal information or payment credentials during Q4, which includes the busiest online shopping periods of the year.

Source: © Justin Paget via www.gettyimages.com

In a brand phishing attack, criminals try to imitate the official website of a well-known brand by using a similar domain name or URL and web page design to the genuine site. The link to the fake website can be sent to targeted individuals by email or text message, redirected during web browsing, or triggered from a fraudulent mobile application. The fake website often contains a form intended to steal users' credentials, payment details or other personal information.

Top phishing brands in Q4 2019

The top brands are ranked by their overall appearance in brand phishing attempts:

1. Facebook (related to 18% of all brand phishing attempts globally)
2. Yahoo (10%)
3. Netflix (5%)
4. PayPal (5%)
5. Microsoft (3%)
6. Spotify (3%)
7. Apple (2%)
8. Google (2%)
9. Chase (2%)
10. Ray-Ban (2%)

Top phishing brands by platform

During Q4 there were significant differences in the brands being used in each phishing vector: for example the focus in the mobile vector was on major technology and social media brands as well as banks, while in the email vector, #2 was part of a shopping phishing campaign before Black Friday in November 2019.

Email (27% of all phishing attacks during Q4)

1. Yahoo
2. Rbs (Ray-Ban Sunglasses)
3. Microsoft
4. DropBox

Web (48% of all phishing attacks in Q4)

1. Spotify
2. Microsoft
3. PayPal
4. Facebook

Mobile (25% of all phishing attacks in Q4)

1. Chase Mobile Banking
2. Facebook
3. Apple
4. PayPal

“Cybercriminals are using a variety of attack vectors to trick their intended victims into giving up personal information and login credentials or transferring money. Although this is often done using spam emails, we have also seen attackers obtain credentials to email accounts, study their victim for weeks and craft a targeted attack against partners and customers to steal money,” said Maya Horowitz, head of Cyber Research and Threat Intelligence of Check Point Research.

“Over the last two years, incidences of this type of attack have spiked with the increased use of cloud-based email, which makes it easier for criminals to disguise themselves as a trusted party. Phishing will continue to be a growing threat in 2020.”