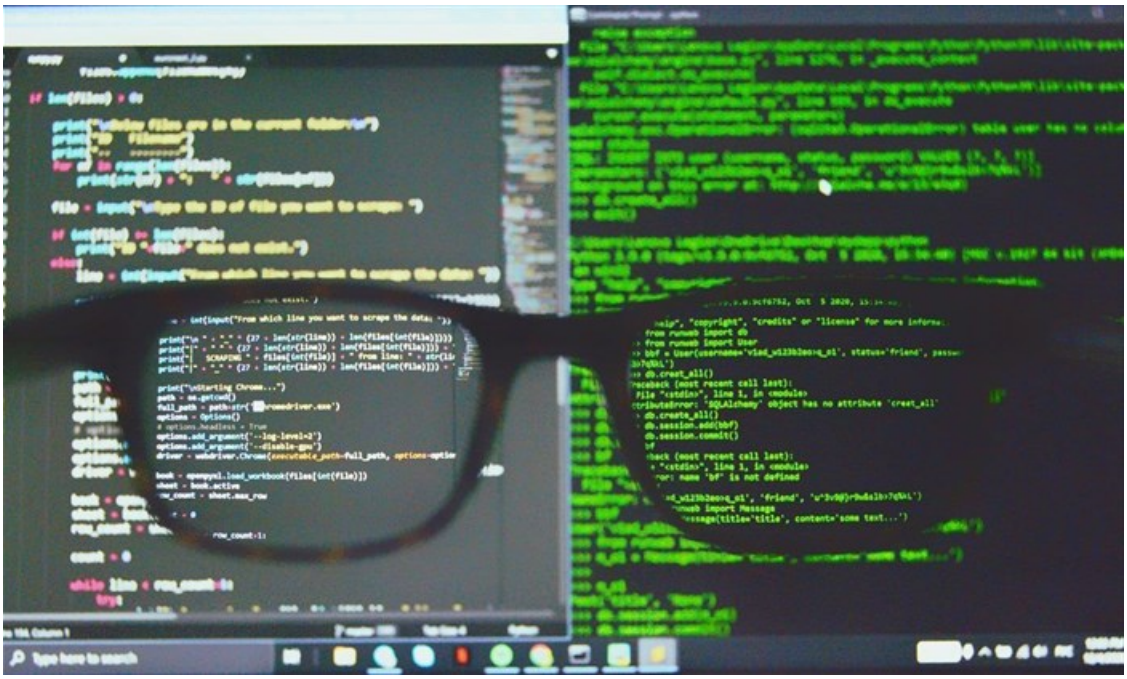
Most imitated brands for phishing attempts in Q2 2021

Check Point Research (CPR) has published its new Brand Phishing Report for Q2 2021. The report highlights the brands which were most frequently imitated by criminals in their attempts to steal individuals' personal information or payment credentials during April, May and June.



Source: Unsplash

In a quarter that saw Microsoft warn of a new Russian Nobelium phishing campaign, the technology giant was again the brand most frequently targeted by cybercriminals, as it was in both Q1 2021 and Q4 2020. Forty-five percent of all brand phishing attempts were related to Microsoft in Q2 (up six points from Q1). Shipping company DHL maintained its position as the second most impersonated brand, with 26% of all phishing attempts related to it, as criminals continue to take advantage of the growing reliance on online shopping.

CPR's latest report also reveals that technology is still the most likely industry to be targeted by brand phishing, followed by shipping and retail. In Q1 2021, retail was interestingly overtaken in the list by banking, but it has now reclaimed its position in the top three possibly owing to the likes of the Amazon Prime Day sales.

USBs are back: Kaspersky uncovers a rare threat campaign

16 Jul 2021

"Cybercriminals are continually increasing their attempts to steal peoples' personal data by impersonating leading brands. In fact, in the run up to Amazon Prime Day in Q2, more than 2,300 new domains were registered about Amazon," said Omer Dembinsky, data research group manager at Check Point Software.

“Unfortunately, it’s the human element that often fails to pick up on misspelt domains or suspicious texts and emails, and as such, cybercriminals continue to impersonate trusted brands to dupe people into giving up their personal information. In Q2, we also witnessed a global surge in ransomware attacks which are often spread initially through phishing emails containing malicious attachments. As always, we encourage users to be cautious when divulging their data, and to think twice before opening email attachments or links, especially emails that claim to be from companies such as Amazon, Microsoft or DHL as they are the most likely to be imitated.”

In a brand phishing attack, criminals try to impersonate 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, a user can be redirected during web browsing, or it may be 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 Q2 2021

- Microsoft (related to 45% of all brand phishing attempts globally)
- DHL (26%)
- Amazon (11%)
- Bestbuy (4%)
- Google (3%)
- LinkedIn (3%)
- Dropbox (1%)
- Chase (1%)
- Apple (1%)
- Paypal (0.5%)