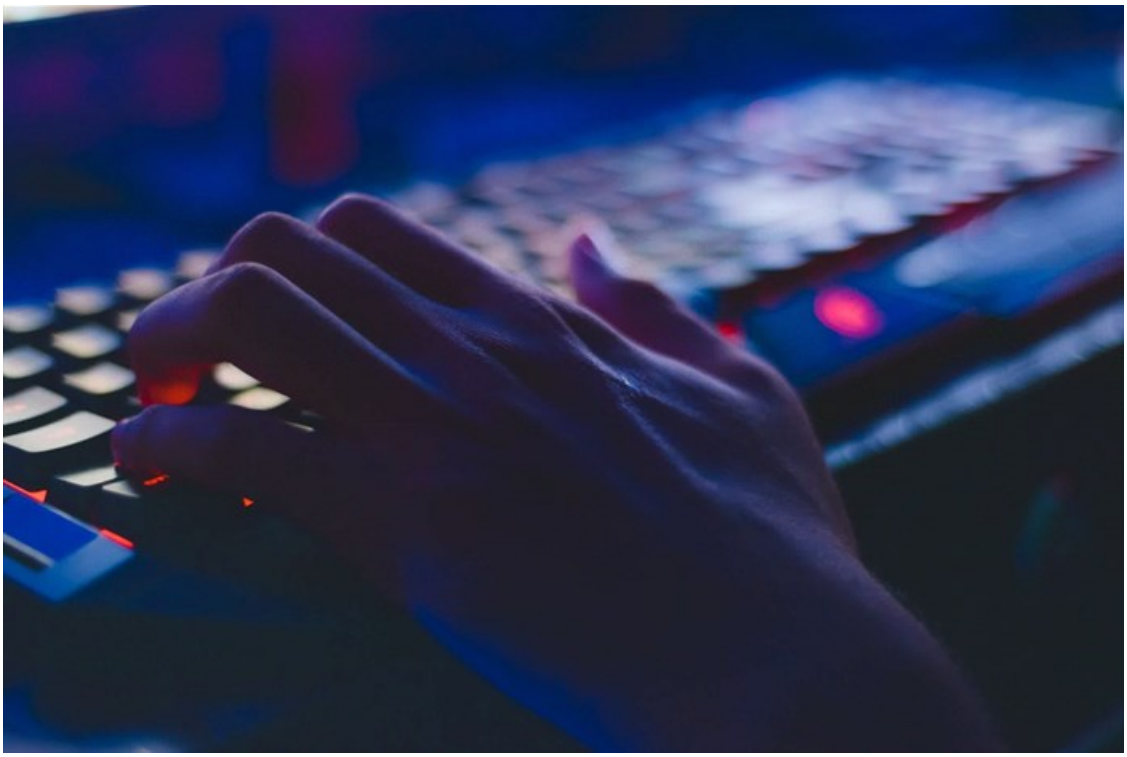
New report reveals the leading brands that hackers imitate the most

Check Point Research (CPR) has published its *Brand Phishing Report* for Q3 2022. The report highlights the brands which were most frequently imitated by criminals in their attempts to steal individuals' personal information or payment credentials during July, August and September.



Source: Unsplash

While LinkedIn was the most imitated brand in both Q1 and Q2 2022, it is the shipping company DHL that took the top spot in Q3, accounting for 22% of all phishing attempts worldwide. Microsoft is in second place (16%) and LinkedIn has fallen into third, making up just 11% of scams, compared to 52% in Q1 and 45% in Q2.

DHL's increase could be due in part to a major global scam and phishing attack that the logistics giant warned about itself just days before the quarter started. Instagram has also appeared in the top ten list for the first time this quarter, following a 'blue-badge' related phishing campaign that was reported in September.

Shipping is one of the top industry sectors for brand phishing, second only to technology. As we head into the busiest retail period of the year, CPR said it will continue to monitor shipping-related scams as threat actors will likely increase their efforts to take advantage of online shoppers.

“Phishing is the most common type of social engineering, which is a general term describing attempts to manipulate or trick users. It is an increasingly common threat vector used in most security incidents,” commented Omer Dembinsky, data research group manager at Check Point.

“In Q3, we saw a dramatic reduction in the number of phishing attempts related to LinkedIn, which reminds us that cybercriminals will often switch their tactics to increase their chances of success. It is still the third most commonly impersonated brand though, so we’d urge all users to stay mindful of any emails or communications purporting to be from LinkedIn. Now that DHL is the brand most likely to be imitated, it’s crucial that anyone expecting a delivery goes straight to the official website to check progress and/or notifications. Do not trust any emails, particularly those asking for information to be shared.”

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, a user can be redirected during web browsing, or it may be triggered by 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 Q3 2022

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

- DHL (related to 22% of all phishing attacks globally)
- Microsoft (16%)
- LinkedIn (11%)
- Google (6%)
- Netflix (5%)
- WeTransfer (5%)
- Walmart (5%)
- WhatsApp (4%)
- HSBC (4%)
- Instagram (3%)