


Social Now Among Top Three Sectors to be Imitated in Phishing Attempts in Q3 2021

 blog.checkpoint.com/2021/10/19/social-now-among-top-three-sectors-to-be-imitated-in-phishing-attempts-in-q3-2021

October 19, 2021

Check Point Research issues Q3 Brand Phishing Report, highlighting the leading brands that hackers imitated in attempts to lure people into giving up personal data

Our latest Brand Phishing Report for Q3 2021 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 2021.

In Q3, Microsoft continued its reign as the brand most frequently targeted by cybercriminals, albeit at a slightly lower rate. Twenty-nine percent of all brand phishing attempts were related to the technology giant, down from 45% in Q2 2021, as threat actors continue to target vulnerable, distributed workforces during the COVID-19 pandemic. Amazon has replaced DHL in second position, accounting for 13% of all phishing attempts versus 11% in the previous quarter, as criminals look to take advantage of online shopping in the run-up to the holiday season.

Our latest Q3 report also reveals that, for the first time this year, social was among the top three sectors to be imitated in phishing attempts, with WhatsApp, LinkedIn and Facebook all appearing in the top ten list of most imitated brands.

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 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 Q3 2021

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

Google Phishing Email – Credentials Theft Example

During this quarter, we witnessed a malicious phishing mail that was trying to steal access credentials to a Google account. The email (see Figure 1), which was sent from the email address **Google (no-reply@accounts[.]google[.]com)**, contained the subject **“Help strengthen the security of your Google Account”**. In the following fraudulent email we notice the year wasn't changed (“2020 Google”). The attacker was trying to lure the victim to click on a malicious link (

275a82a80541[.]jeastus[.]cloudapp[.]azure[.]com) which redirects the user to a fraudulent malicious login page that looks like the real Google login website (see Figure 2). In the malicious link, the user needed to enter their Google account details.

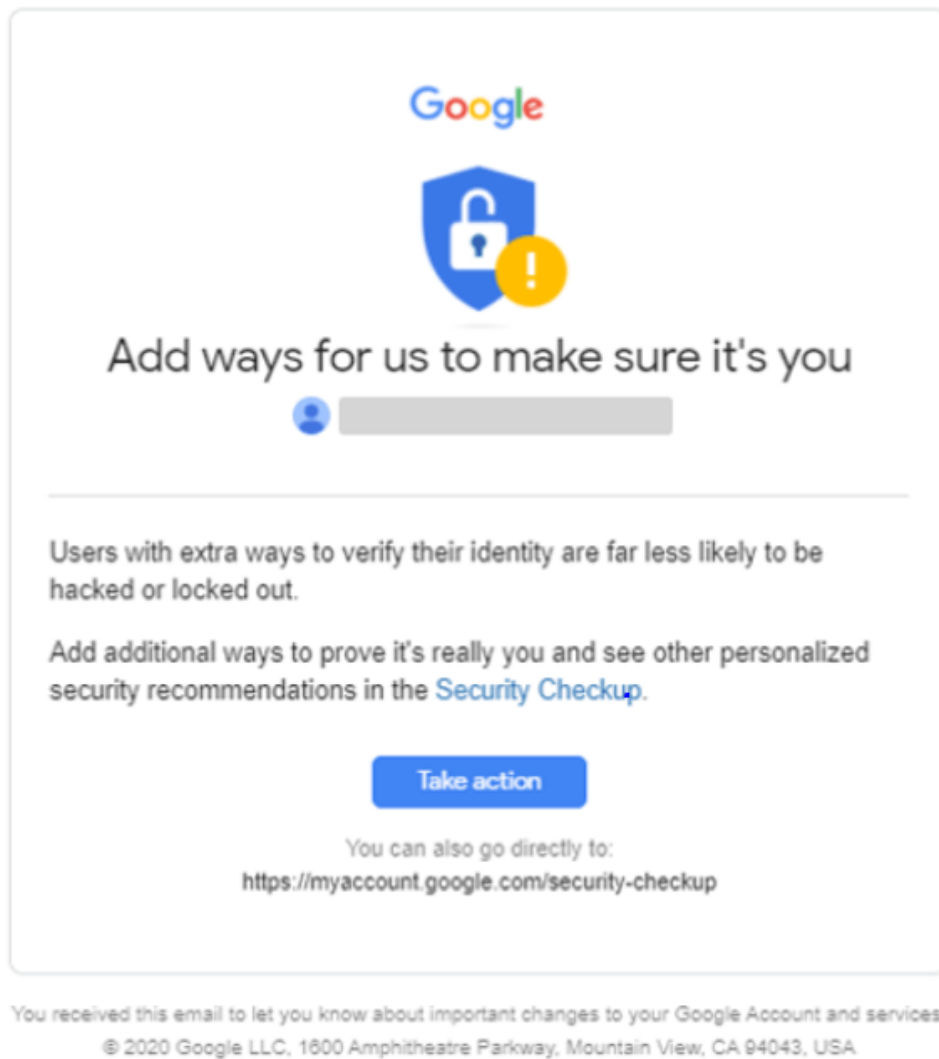


Figure 1: The malicious email which was sent with the subject “Help strengthen the security of your Google Account”

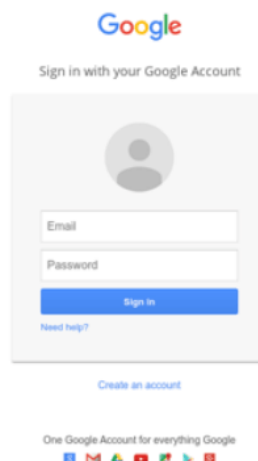


Figure 2: fraudulent login page

[http://router-ac1182f5-3c35-4648-99ab-275a82a80541\[.\]eastus\[.\]cloudapp\[.\]azure\[.\]com](http://router-ac1182f5-3c35-4648-99ab-275a82a80541[.]eastus[.]cloudapp[.]azure[.]com)

LinkedIn Phishing Email – Account Theft Example

In this phishing email, we see an attempt to steal a user’s LinkedIn account information. The email (see Figure 1) which was sent from the email address **LinkedIn (linkedin@connect[.]com)**, contained the subject **“You have a new LinkedIn business invitation from *****”**. The attacker was trying to lure the victim to click on a malicious link, which redirects the user to a fraudulent LinkedIn login page (see Figure 2). In the malicious link ([https://www\[.\]coversforlife\[.\]com/wp-admin/oc/nb/LinkedinAUT/login\[.\]php](https://www[.]coversforlife[.]com/wp-admin/oc/nb/LinkedinAUT/login[.]php)), the user needed to enter their username and their password. On the fraudulent website we can see that the year wasn’t changed (“2020 LinkedIn”)

LinkedIn Business Invitation

You have a new business invitation from [REDACTED]
*Status: **Verified Member**

Message:

Hi [REDACTED],

Please do you still have this products in stock, we would like to place and order?
Kindly reply me with your contact so i can send you details and specification about the order.

[View Contact Details](#)

This message was sent from LinkedIn.com mail server to [REDACTED]

© 2021 LinkedIn Ireland Unlimited Company, Wilton Plaza, Wilton Place, Dublin 2.
LinkedIn Ireland Unlimited Company

Figure 1: The malicious email which was sent with the subject **“You have a new LinkedIn business invitation from *****”**



Welcome Back

Welcome back. Sign in to discover what your clients and business partners want.



Confirm Account

**** · Not you?

Password Show

Sign In

Sign in using one-time sign in link

[Forgot password?](#)

New to LinkedIn? [Join now](#)

LinkedIn © 2020 [User Agreement](#) [Privacy Policy](#) [Community Guidelines](#) [Cookie Policy](#) [Copyright Policy](#) [Send Feedback](#)

Figure 2: fraudulent login page

[https://www\[.\]coversforlife\[.\]com/wp-admin/oc/nb/LinkedInAUT/login\[.\]php](https://www[.]coversforlife[.]com/wp-admin/oc/nb/LinkedInAUT/login[.]php)

As always, we encourage users to be cautious when divulging personal data and credentials to business applications or websites, 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 impersonated.