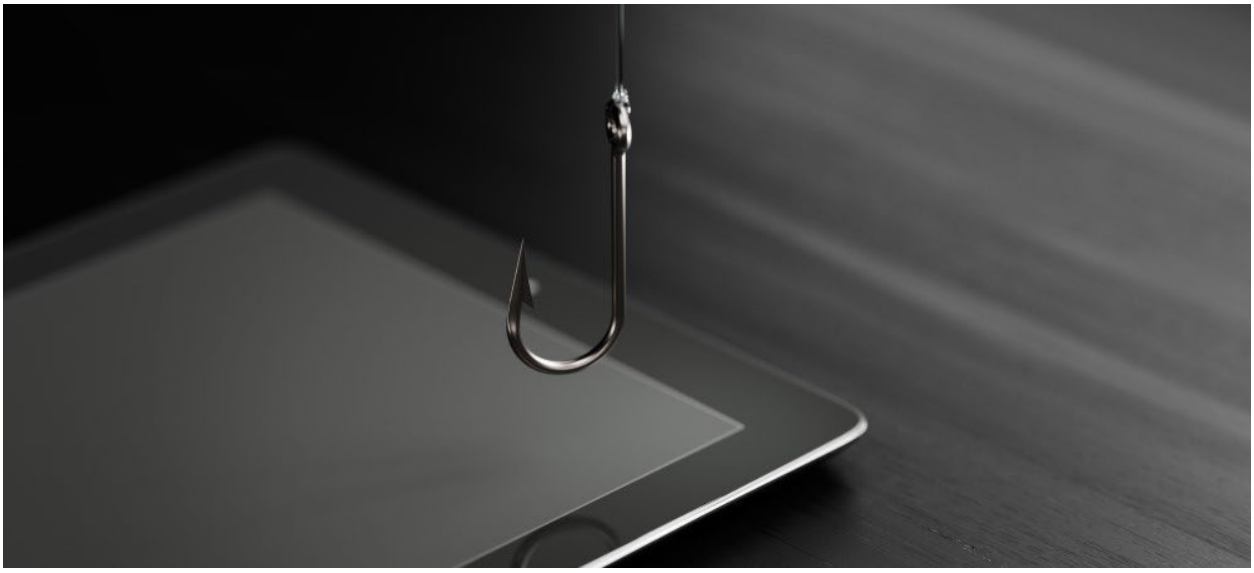
CYBERSCOUT
A TransUnion® Brand

april

Phishing Scams: How to Protect Yourself

By: Eugene Bekker



Imagine you're waiting in line for coffee and your phone starts going off. You suddenly get two text messages, an email and a missed call – all from your bank saying they suspect fraudulent activity on your account. They've put a hold on your accounts for security reasons and urge you to contact them to unlock the accounts.

You want to follow up, but something doesn't feel quite right.

Given the explosion in social engineering attacks like phishing, vishing or smishing scams, it's wise to be skeptical of urgent and unexpected emails, phone calls and text messages you receive. The 2021 Data Breach Investigations Report (DBIR) notes that more than one-third (36%) of all data breaches involve phishing.

The pain of those breaches is real: The FBI's Internet Crime Report found that phishing, vishing and smishing were the No. 1 reported cybercrime last year, costing victims more than $54 million in damages.

For the individual whose mobile device is getting overwhelmed, though, the question is often simple: *"What can I do?"*

CYBERSCOUT
A TransUnion® Brand

april

POPULAR PHISHING SCAMS

Analysis by Cofense Intelligence found 70% of phishing incidents involve information stealers and keyloggers, which are types of malware programs that secretly gather information from your computer, enabling fraudsters to swipe your credentials.

A common phishing email scam involves a message saying there was suspicious account activity and, to unlock your account, you must provide personal information. Once you provide this information, the phisher can use it to clear out your bank accounts or make fraudulent purchases using your credit card. (A "smishing" scam follows the same logic, except the scammer's mode of contact is via a text message.)

The most important thing to remember is this: Legitimate companies will never ask you to provide your personal information via email or text. They won't call you and ask for it either. If you get such a message, immediately recognize it as a scam and delete it.

Financial institutions may notify you that they had to freeze your accounts based on suspicious activity, but then they'll instruct you to unlock them. Rather than asking for your credentials, they'll typically ask you to log into your online account over a secure internet connection to verify the transactions.

BEWARE OF PHISHING SCAMS

The moral of this story is if you ever get an email, text or phone call stating that there has been suspicious activity on an account, be on alert.

1. Never click on the link provided in the email, and don't call any phone numbers they've provided. Instead, visit the organization's official website and contact the customer service number listed there. Alternatively, you can call the number listed on the back of your bank or credit card.
2. Put your phone number on the Do Not Call Registry to avoid phone calls from scammers.
3. Set up your email inbox to filter out spam and phishing mail.
4. Hover your mouse over every link to verify it is going where you expect it to before you click.
5. Remember, imposter scams are the No. 1 type of reported fraud. In addition to phishing and smishing, these attacks also take the form

of vishing (or voice phishing) where someone is impersonating the IRS, police, your bank or other forms of authority.