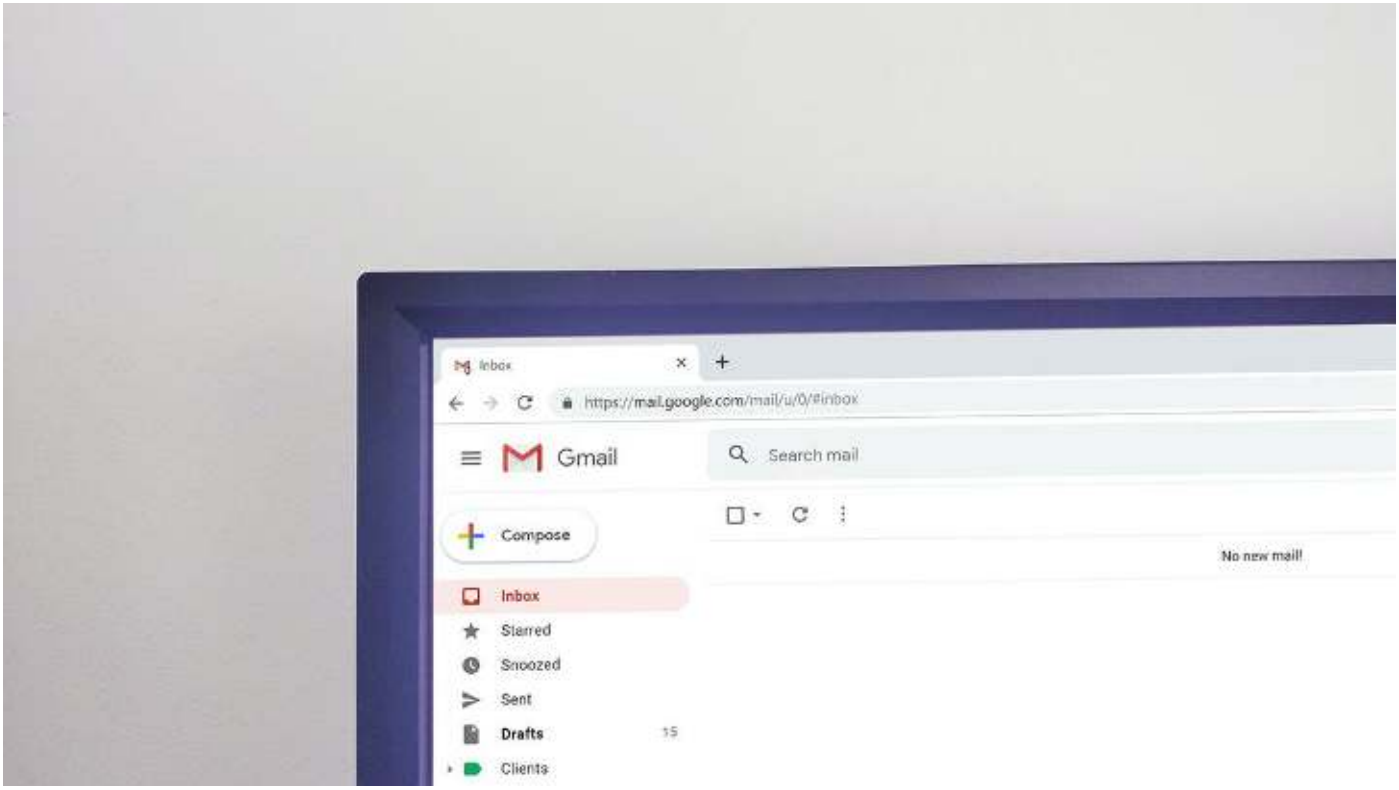
What Is Clone Phishing? Definition, Examples, and Prevention



Phishing attacks come in various shapes and sizes. Almost always they're in the form of communication by a dubious source claiming to be someone you're familiar with, such as a delivery company, bank, or a money-sending site. The purpose is to get you to enter your password, credit card details, or anything else that can be used to access your personal or financial resources.

Clone phishing is a form of phishing attack that uses cloned emails or web pages to trick people into entering these details. Before you know it, they've clicked the wrong link, entered the wrong information, and their accounts have been hacked or their bank balance is disappearing.

These scams can hit almost anyone, anywhere, and without some vigilance and the knowledge of some of the red flags, they could happen to you. Fortunately, they're relatively easy to avoid if you know what to look for. So, let's go into exactly what clone phishing is and how you can avoid it happening to your or your loved ones.

Clone Phishing Definition

Cloned web pages or emails are surprisingly easy to make. Usually, a clone phishing scam sends out a communication disguised as a legitimate company or familiar contact.

This may come in the form of an email from a reputable site that you're a member of or even a note in your inbox from a colleague's email address at work. At home, it might be an email disguised as being from Amazon.com, asking you to reset your password. At work, it might come from upper management or Payroll asking you to authorize an emergency payment or provide bank details.

From these impersonated accounts, a scammer is able to extract information from their targets and ultimately use them to get money out of them or to extend the scam until they reach somewhere they can.

The goal of clone phishing is to get around your natural suspicions and create an innocent-looking attack that you don't see coming. So, how do they get under your radar? Let's take a look at some of the common structures of a clone phishing attack.

Structure of a Clone Phishing Attack

Social media and emails are two of the common medium for clone phishing attacks. Usually, the process begins with a cloned web page sent to addresses *en masse*.

These emails pretend to be from a reputable source and encourage the recipient to click on an embedded link. This link either allows phishers to receive entered personal details from the target or installs malware on their device that gives the phisher these details.

Once a legitimate correspondence with the target has been discovered by the hacker, the path for clone phishing becomes apparent. Hackers can clone the identity of a trusted correspondent and send further emails under that guise. They can also access the contacts of the initial targets and spread from there, infiltrating offices, schools, and other organizations through the emails on this contact list.

Once they're in, they'll pretend to be someone you know, typically reference a conversation you previously had, and request some details from you, or a change of plan that bypasses a security measure.

The majority of victims of clone phishing are attacked through social media and over half of them were attempting to get to the credit card or bank details of the recipient.

Examples of Clone Phishing

Usually, a clone phishing scam works by referencing an email that was previously sent. For example, let's say that you've been dealing with a colleague in another department via email for the last few days and you're in the process of authorizing a delayed payment to them. A clone phishing email could look something like this:

Hi [You]

As a correction to the previous email, I'd like to let you know the bank details for the payment have changed. Please see updated details for this the deposit of this month's payment.

Don't worry about authorization, I'll clear that up from this side. We now urgently need the payment to be made by E.O.D. please.

Bank Account Number: [hacker's bank]
Payment Code: [Hacker's bank]

Kind Regards,

[Name of colleague]
[Hacker's number/contact]

As you can tell, it's an easy trick to fall for, and can cost you or your company a significant amount of money. Fortunately, there are some basic principles of cybersecurity to follow when dealing with people online, and these can dramatically reduce the chances of you falling victim to one of these scams.

Clone Phishing Protection Methods

There are some safety basics when dealing with phishing scams of any kind. Here are some that are particularly useful for avoiding clone phishing attempts.

- One easy way to spot a fake email is by the use of poor spelling or grammar. Many scammers come from non-English speaking countries and run their projects from the other side of the planet. If your email looks hastily formed, be suspicious.

- Similarly, if an email has a sense of urgency, for example, telling you that you have 24h to pay a fine, or a subscription, consider that suspect too. Many of these scams work by giving you little time to think, and rushing you into a mistake.

- If the email is from someone you know, and it tells you to keep the process a secret from other colleagues, this can also be a red flag.

- If it tells you to click a link or open an attachment, be very cautious.

- If the contact details are provided in the email, don't use them! Find the contact details you have for them already and use those to check with the sender.

- Always follow set policies and procedures when working within the company. If an email tells you to do something that is confidential and outside of common policy, there's a good chance it's a scam.

- Never assume a phone call is genuine. Make sure that if you need to give secure details, you first call them back on an established number to do it – not on a number the caller is giving you!

- Use MFA: multifactor authentication. This means that in order to log into an account, the user needs to access a text message or call to their device, meaning that it's impossible for someone without your phone or tablet to get in, even if they do get your login details.

In general, if you receive an email from someone you know and the character, spelling, or tone of the email seems off, check to see if there's any obvious way it could lead to an impersonator getting your details. If you're suspicious, contact the owner of the email account on a different medium, via an established channel, like a saved phone number.

For a more in-depth approach, consider the 4 levels of mitigation:

- Make it difficult for scammers to get in
- Help users identify and report scam emails
- Protect your organization from their effects
- Respond quickly to any incidents that arise

If this sounds complicated, it might be a good idea to assess your cybersecurity risk by using a cybersecurity risk rating by SecurityScorecard. With it, you'll be able to understand the principles of cybersecurity and how you and your vendors sit on the spectrum of safe to vulnerable. SecurityScorecard can also help you test your security controls and accurately monitor potential threats.

Conclusion

Clone phishing is an advanced phishing attack, and as scammers get sharper to people's defenses, these attacks are bound to get smarter. These particular attacks take advantage of trust within or between organizations and exploit the good nature of people to trick them into going against common policies.

Thankfully, there are cybersecurity basics that are easy to follow, and failing that, cybersecurity experts are happy to help with security assessments.

For more information on that, check out SecurityScorecard's available services.