What is Phishing? Recognize, Report & Avoid Phishing Scams

Phishing targets personal data that can be “fished” online. From private conversations to financial data and even access to bank accounts, from personal photos to search history or details of online behaviour – all of this is valuable to users, but also to hackers trying to mislead users into obtaining it.

What is Phishing?

Phishing is a type of online fraud that relies on social engineering attacks to trick users into divulging their sensitive information including credit card numbers and login credentials by impersonating a trustworthy entity. Phishing is usually carried out via email, SMS, or instant messaging applications through a dangerous link. But phishing links can also be snuck into messages posted on social networks, bulletin boards, etc.

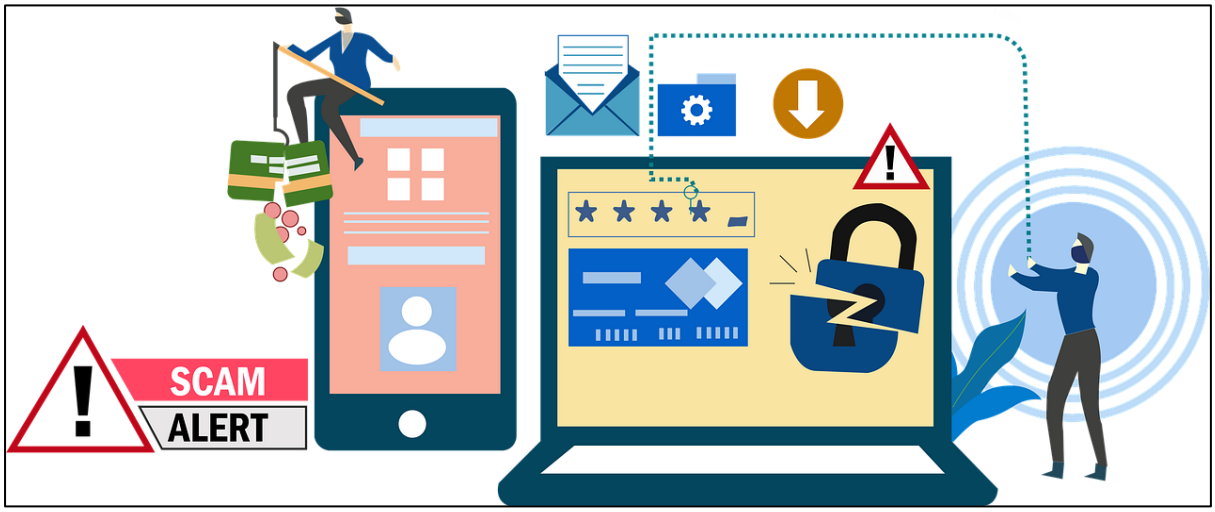
Phishing scams are the most efficient attack vector for bad actors to steal sensitive information. Even though attackers have plenty of options, they prefer phishing because it does one thing better than any other method: it tricks victims into partaking in their own attack.

How Does a Phishing Attack Happen?

A classic phishing attack starts with an e-mail or SMS purportedly from your bank, your e-mail service provider, or another reputable company you have signed up with. These messages usually require that you follow a link to validate some personal information. Failure to comply will lead to account suspension or termination. To gain credibility, a phishing message usually includes logos and visual identities ripped off from the impersonated entity. Instead of taking you to the bank’s webpage, though, the link points to the fraudster’s website. Anything you fill in will be sent to the attacker and used to illegally access the account. Once the account is compromised, the attacker can abuse it in various ways, depending on what type of account that is. In the case

of an e-banking website, a hacker could make payments or transfer money from the user's account. An e-mail account can be used to gain access to private conversations or send spam to other users and so on.

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.



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.

Common phishing email scams involve 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" (SMS + phishing) scam follows the same logic, except the scammer's mode of contact is via a text message.

Signs & Examples of a Phishing Email

As you encounter more phishing messages, you will learn to identify them with just a quick look. Usually, these messages are rife with spelling errors. This mostly happens because the attacker is not a native English speaker. The message is also impersonal and generic. It often starts with "Dear user" rather than your username or full name. Unlike legit messages from the service provider, phishing messages don't mention your full name or username. They are designed to trick every recipient, not just you and the attackers do not know who you are. They just hope you have an account on the respective service. The link you are supposed to follow is also different from the URL you enter in your browser when you access the respective service. Often the URL starts with an IP address.

Some of the most lucrative phishing emails pretend to come from Apple Inc. in Cupertino, California. The operators behind these campaigns have honed their skills to create messages that are nearly indistinguishable from Apple's graphics. Thus armed, they dupe thousands of unwary users into handing over their passwords and credit card data, thinking they are communicating with the actual help desk at Apple. In fact, they are handing over their precious data to attackers. As the screenshot below shows, the message instills fear saying your account has been compromised, that Apple has locked it "for security reasons", and that you now need to re-enter all your data to confirm you're you and not the hacker.

A typical phishing email

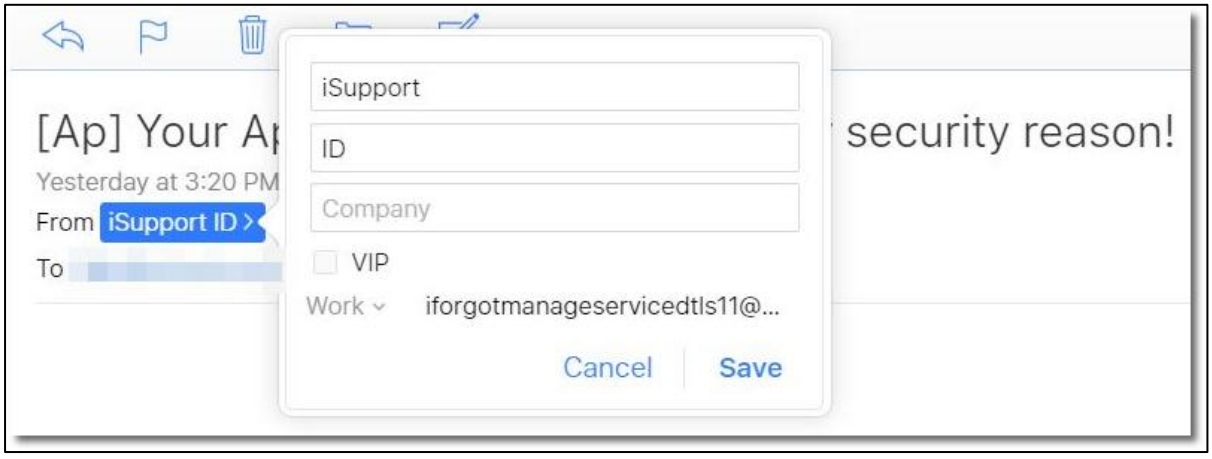
The message is crafted well enough to trick the untrained eye, but a few telltale signs show we are being scammed here.

Clue #1: “user@icloud.com has been temporarily disabled”

Ask yourself this: How is my account disabled if I’m getting this on my current iCloud email account, which I can still access with my current Apple ID and password just fine? Something’s not right here.

Clue #2: email sender

Scammers will usually try to mimic the email address of the company they are impersonating. In this case, they used the iconic “i” moniker typically found in Apple nomenclature. This is meant to both add credibility and avoid anti-phishing mechanisms. Clicking on the address name also reveals the actual address the email comes from. The address “iforgotmanageservicedtls11@personalverfctioninfos.com” hardly sounds like the real Apple in Cupertino.



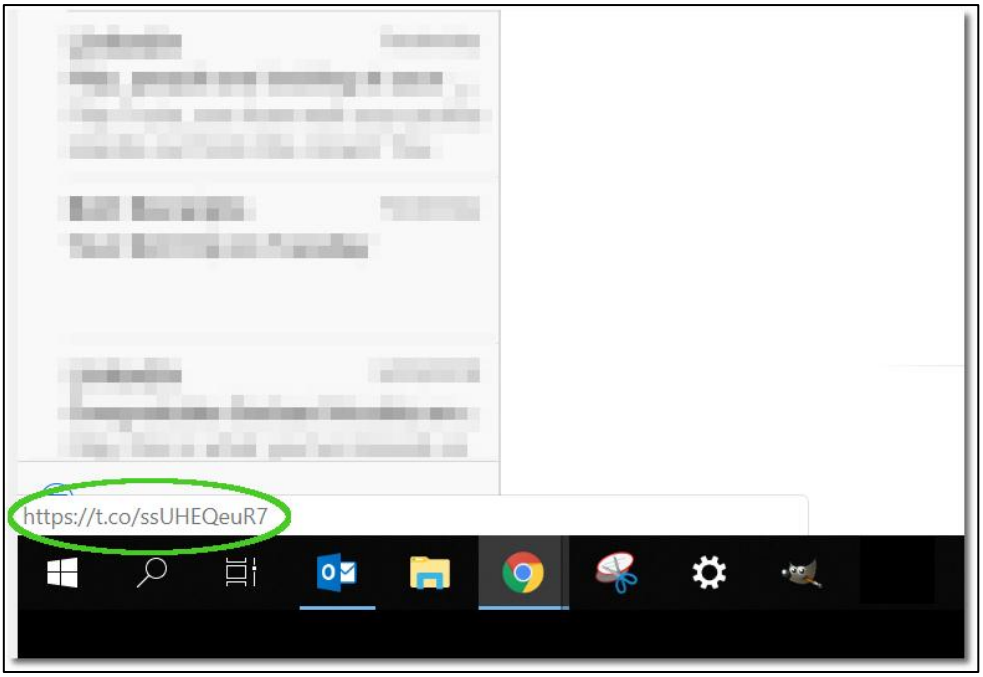
For any other service or company, the attackers might impersonate, check previous legitimate emails to see what the real address looks like.

Clue #3: “Your Apple ID has been locked for security reason”

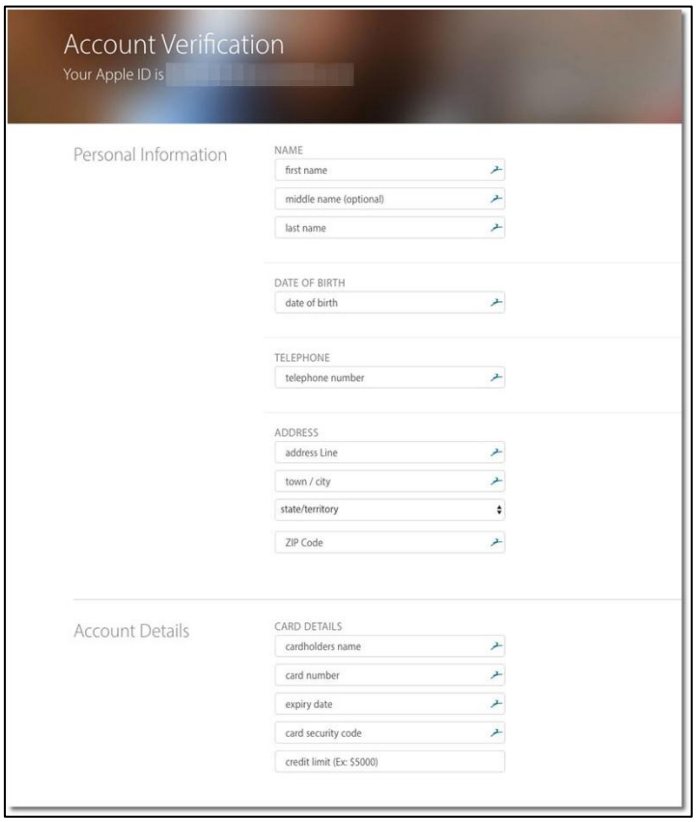
Typical scareware subject line. Phishing scams try to frighten you by saying something has gone wrong and you need to take IMMEDIATE action. It’s a classic clue that you are dealing with a swindle. And shouldn’t “reason” be in plural here? Poor English is always a sign you should be wary.

Clue #4: “go HERE” doesn’t take you to Apple’s website

Hover your mouse cursor over any hyperlink and you will see the actual URL without having to click on it. In this example, iCloud Mail is open in Chrome, which reveals the URL in the bottom left-hand corner of the browser’s window. Microsoft Outlook reveals the URL in a square bubble, right above the mouse cursor.



The first thing to notice here is that the URL has been shortened. No legitimate company, particularly Apple, will ever do that. But, say you don't notice this and proceed to click on the link. Typically, you'll be taken to a page designed to look like it's Apple's website. Chances are the page will host a form asking you to enter your personal data, and sometimes even financial data. Don't do it! Apple will never ask you to do any of this, even if your account does get hacked.



Example of a fake form – Phishing Scam

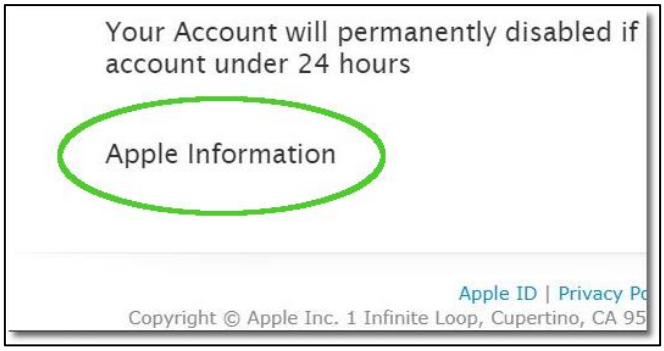
Clue #5: "Your Account will permanently be disabled if you do not verify your account under 24 hours"

Another dose of scareware, just in case the first attempts misfired. No company will EVER permanently disable your account simply on the basis that it got hacked. Quite the contrary. They will try to fix it and get you back on track.

We're also missing a verb here. Nice try guys!

Clue #6: email signature

Big companies like Apple, Facebook, and Google typically sign emails using nothing more than the company name. Some might contain terms like "Support" or "Team," etc. This varies by company. But "Apple Information?"



That doesn't sound like much of a department name, does it? In fact, it almost sounds like the scammers were running out of ideas.

When in doubt, look for the last legitimate email from your vendor and compare the signatures. If they don't match, you know what's going on.

Clue #7: no URL where there should be one

The words *Apple ID* and *Privacy Policy* may seem hyperlinked. In fact, they are fake hyperlinks that don't go anywhere. Another sign that something is off. A "Privacy Policy" is meant to be accessible for the customer to review the rights and obligations of all parties involved.

Here, we are looking at an incomplete replica of Apple's template:

This is a classic example of how phishing scammers operate. These campaigns are a dime a dozen, and almost each one brings something new to the table.

How do I Stop Getting Phishing Emails & SMS?

Anti-phishing defenses are layered mechanisms.

1. The first line of defense is the spam filter: a feature that is usually integrated with your security solution and that filters junk e-mail from legit messages. A good antispam filter blocks the phishing attempt in its early stage, so you don't even see the lure that is being thrown at you.
2. The second line of defense is a good scam filter for your Android smartphone. Scam filters monitor incoming SMS messages in real-time and alert you when a dangerous link arrives in a text message on your phone.
3. The third layer of defense is the anti-phishing or anti-fraud module – another component of the anti-virus that analyzes the web page you land on and determines whether it has been designed to steal your data. Even if you have fallen for the scam and opened the phishing message, the anti-phishing module should prevent you from filling in the form with your sensitive information (credit card number, expiration date, CVV, or PIN number, among others).
4. Last, but not least, setting up two-factor authentication for the accounts that support it ensures that, even if somebody gets your login credentials, they couldn't log in without a secondary password sent by the service on your mobile device or token. We have this great tutorial on how to set up 2-factor authentication for the most popular web services.

What to do if You Receive a Phishing Attempt

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?

Use Bitdefender Scamio to check suspicious messages, images, or links for free:

https://www.bitdefender.com/consumer/scamio

Use your best judgment as well. The moral of the 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. As a rule of thumb, never hand over your personal data, password, or credit card information to an email sender before you thoroughly verify, they are who they claim to be.

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. 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 advise you to log into your online account over a secure internet connection to verify the transactions. If you get such a message, mark it as spam and delete it. That's not to say you should consider every warning message a scam. Just be sure to investigate thoroughly before you take any action that you might regret later.

To prevent Phishing Scams:

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. Enable Bitdefender Antispam on Windows computers that use Microsoft Outlook and Mozilla Thunderbird. As far as Apple users are concerned, if you receive what you believe to be a phishing email purporting to be from Cupertino, Apple recommends forwarding the message with complete header information to reportphishing@apple.com so that the company can investigate the matter.
4. Hover your mouse over every link to verify it is going where you expect it to before you click.
5. Bear in mind, 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.

What to Do if you Responded to a Phishing message

If you've fallen victim to a scam and have provided your password, bank details, Personally Identifiable Information (PII), or other sensitive personal information, the scammer already has your data.

Depending on what information was disclosed, take these actions immediately:

1. Change the password of the account – email, social media, etc. – you provided information about. If you use the same password elsewhere, change that, too. If you struggle to remember all your passwords, you might benefit from using a password manager.
2. If you've given a fraudster your bank details, contact your bank right away and explain that you're the victim of a scam.
3. Report the scam to the proper authorities if you paid someone you believe to be a scammer, gave away personal information, or if they have access to your devices.