PHISHING/SCAMS

Phishing

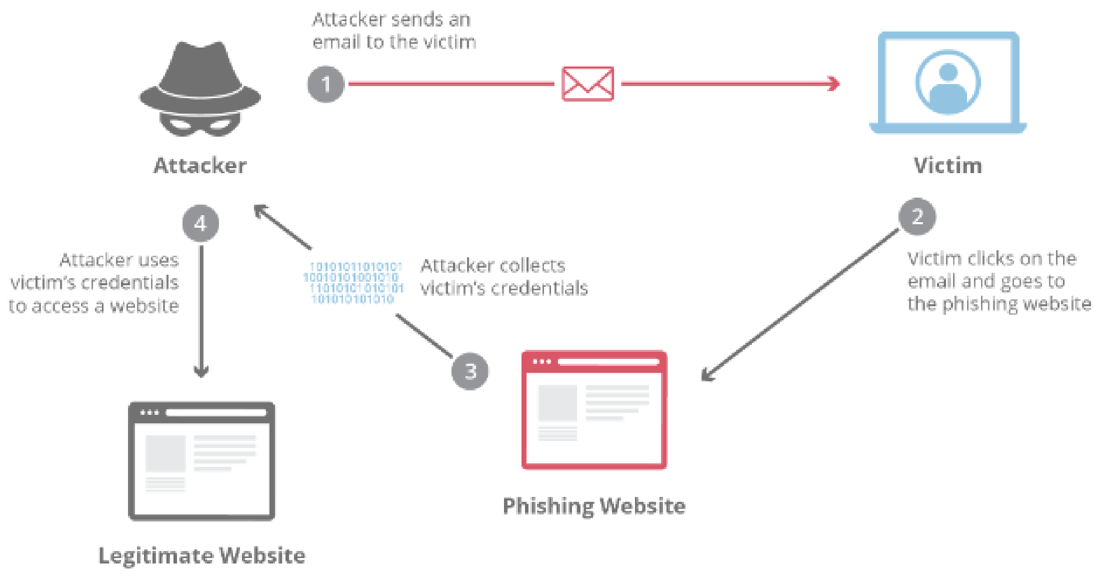
Phishing is the fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

There are also different types of phishing attacks to include; “Spear phishing,” “Clone phishing,” and “Smishing.”

“Spear phishing” is a highly targeted attack that uses personalized messages to deceive specific individuals, organizations, or roles within a company. The goal is to steal sensitive information or infect the target's device with malware.

“Clone phishing” is where an attacker duplicates a message that the target has previously received, such as a mass email from a brand or a fake tracking email. The attacker then uses the replicated message to deceive a broad range of targets.

“Smishing” is a social engineering attack that uses fake text messages to trick people into sharing sensitive information, downloading malware, or sending money to cybercriminals. The victim is usually asked to click a link, call a phone number, or contact an email address provided by the attacker.


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
3
Attacker collects victim's credentials
4
Attacker uses victim's credentials to access a website
Phishing Website
Legitimate Website

Phishing attempts usually occur through emails and messaging apps. That is why it is important to never click on a link, or a message, from someone you don’t know. Phishing is the most common data breach vector, accounting for 16% of all breaches.

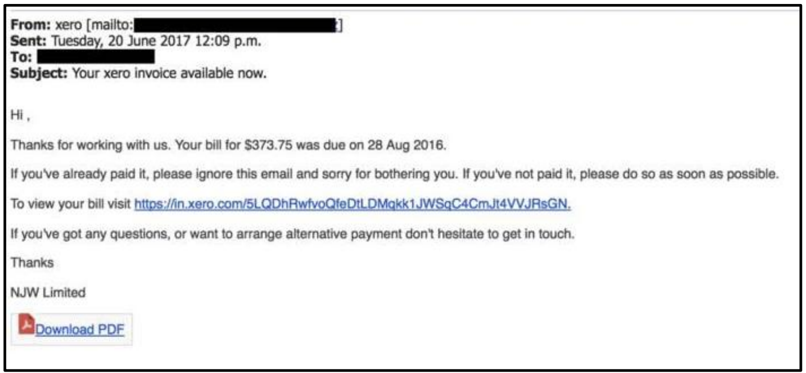
PHISHING/SCAMS

Before you click / preventative measures

If the link you just received, or the sender of the link, is suspicious, don’t click the link or even open the message. To determine if it’s a “phishing” attempt, look at inconsistencies in the senders information, link and domains. A lot of emails or messages will have spelling errors, or some of the letters may look a little off. You can also hover your cursor over the link to preview the URL that it leads to. If the domain doesn’t exist, its likely a phishing attack. Make sure you are using an email system that has “Phishing Email Detection.” This will usually flag the email and let you know the contents could be dangerous before you click them.

Types of Scams

The Invoice Phishing Scam is very popular. Attackers will send you an email with a past due amount you need to pay. This creates a sense of urgency in people to click the link and pay the amount.



From: xero [mailto:[redacted]]
Sent: Tuesday, 20 June 2017 12:09 p.m.
To: [redacted]
Subject: Your xero invoice available now.

Hi ,

Thanks for working with us. Your bill for $373.75 was due on 28 Aug 2016.

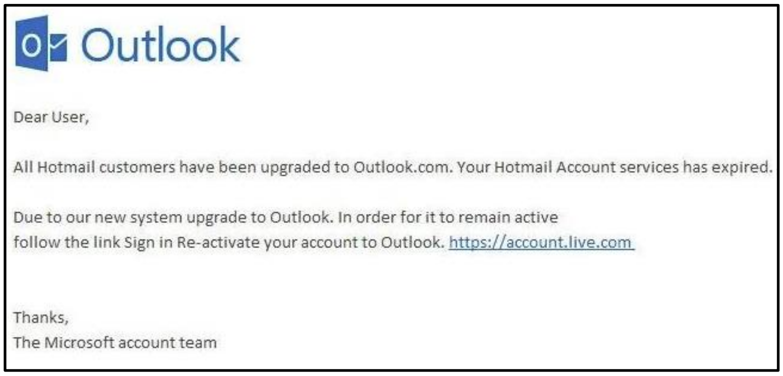
If you've already paid it, please ignore this email and sorry for bothering you. If you've not paid it, please do so as soon as possible.

To view your bill visit https://in.xero.com/5LQDhRwfvoQfeDtLDMqkk1JWSqC4CmJt4VVJRsGN.

If you've got any questions, or want to arrange alternative payment don't hesitate to get in touch.

Thanks

NJW Limited



Dear User,

All Hotmail customers have been upgraded to Outlook.com. Your Hotmail Account services has expired.

Due to our new system upgrade to Outlook. In order for it to remain active
follow the link Sign in Re-activate your account to Outlook. https://account.live.com

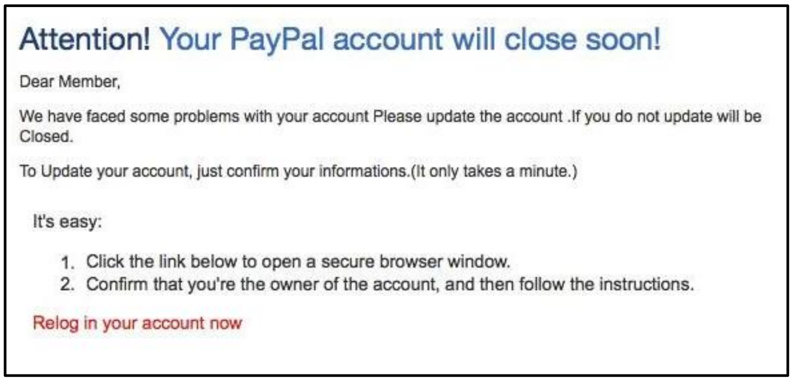
Thanks,
The Microsoft account team

Types of Scams

The email account upgrade is popular as well. The attackers pose as Micorosoft or Google to try to get you to click the link. Nothing visually looks off in this email, that’s why its important to hover over the link.

Types of Scams

The Paypal scam is also popular. The attackers will send you an email posing as paypal, saying you need to re log into your account before it closes. Once you do, they get access to your account.



Attention! Your PayPal account will close soon!

Dear Member,

We have faced some problems with your account Please update the account .If you do not update will be Closed.

To Update your account, just confirm your informations.(It only takes a minute.)

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm that you're the owner of the account, and then follow the instructions.

Relog in your account now

PHISHING/SCAMS

Accidentally clicking on a link / Recovery

If you accidentally click on a “Phishing” link, Malware will likely be downloaded to your device. The types of malware can vary, but it can be anything from key-loggers to spyware. It will be any type of virus that can garner information from whatever device you used to click the link. Another possibility of clicking on a link is it will direct you to a “spoof” website, which will look identical to the real one. A common “Phishing” attempt is posing as Amazon or Apple, and sending you a link to what looks like the Amazon or apple store so that you will enter your information.

If you happen to click on the link, take the next steps as listed below:

1. Disconnect your device from the internet

This can prevent any malware from being able to fully download on your device, and also prevent other devices connected to the same network from being potentially infected.

2. Scan your device using antivirus software

An antivirus is a program that can be installed on your device that prevents, detects, and removes known malware and viruses. If you didn’t already have one downloaded on your device, you will have to do that. Before you connect back to your internet to download it, make sure other devices aren’t connected to the network and that your routers software is the most up to date. However, antivirus programs are not foolproof, some malware is very complex and can slip past antivirus application. So just because your application doesn’t detect it, doesn’t mean it isn’t there. Monitor your network and device for a few days to make sure there isn’t any suspicious activity

3. Change your passwords immediately on a separate device and network

If you already typed in your information to a “Spoofed” site or if the malware has been running long enough, the attackers likely have your information. You will need to immediately change your account passwords to gain control back over the accounts. A great way to stop them from being able to have access to your account is having “Multi-Factor Authentication” enabled. That way if they get your password, they will still need the other form of verification to get into your account.

4. Contact the appropriate parties

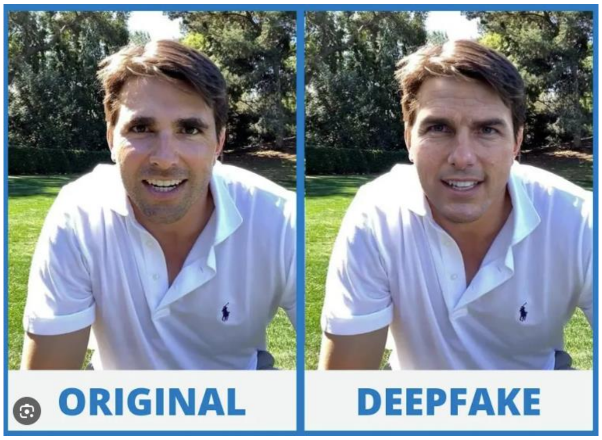
If you accidentally clicked a phishing link or fell for a scam, it might be in your best interest to let your bank know. That way they can also monitor any suspicious transactions associated with your account. You can also get in contact with the Federal Trade Commission (FTC). You can reach them at “https://reportfraud.ftc.gov/assistant” and if it was a phishing email you can forward it to reportphishing@apwg.org

“Phishing” attackers are getting more complex and harder to detect. The emails and messages they send are getting harder to differentiate from legitimate emails. It is recommended you always use caution with regards to emails and messages from non-trusted sources.

PHISHING/SCAMS

Deepfake

One of the newest, and best scams currently is using AI “Deepfake” technology. A “Deepfake” is a video of a person in which their face, body, and voice has been digitally altered so that they appear to be someone else, typically used maliciously or to spread false information. Attackers will pose as someone; possibly a boss, friend, or loved one, and can contact you using a video conferencing app to convince you to either send money, or give up personal information. This has been very popular among dating apps, where people will pose as someone online, facetime them to “Confirm they are real,” and then get money from them.



Deepfake

Deepfakes are created by training deep learning algorithms on large datasets of images and videos. These algorithms learn to mimic the facial expressions, movements, and speech patterns of the target individual, allowing for the creation of highly realistic videos.

You can spot “Deepfake” videos by looking for the following signs:

1. Look for inconsistencies such as unnatural facial movements or mismatched audio.
2. When watching videos, it is important to be cautious about the quality. Look out for blurry spots, unnatural blinking, or no blinking, as well as frequent changes in the background and lighting
3. If you have any suspicions, verify the identity of the person you are talking to in situations like this to ensure you know who they are
4. The caller requesting money, usually urgently and through a hard to trace method like a wire transfer, gift card, payment app, or cryptocurrency.

A Chinese finance worker paid out $25 million dollars to a scammer using deepfake AI technology after they believed they were on a video call with their chief financial officer and other colleagues. He had doubts when he saw what looked like a “Phishing” email, but put aside those doubts after the video call because everyone in the conference looked and sounded real.