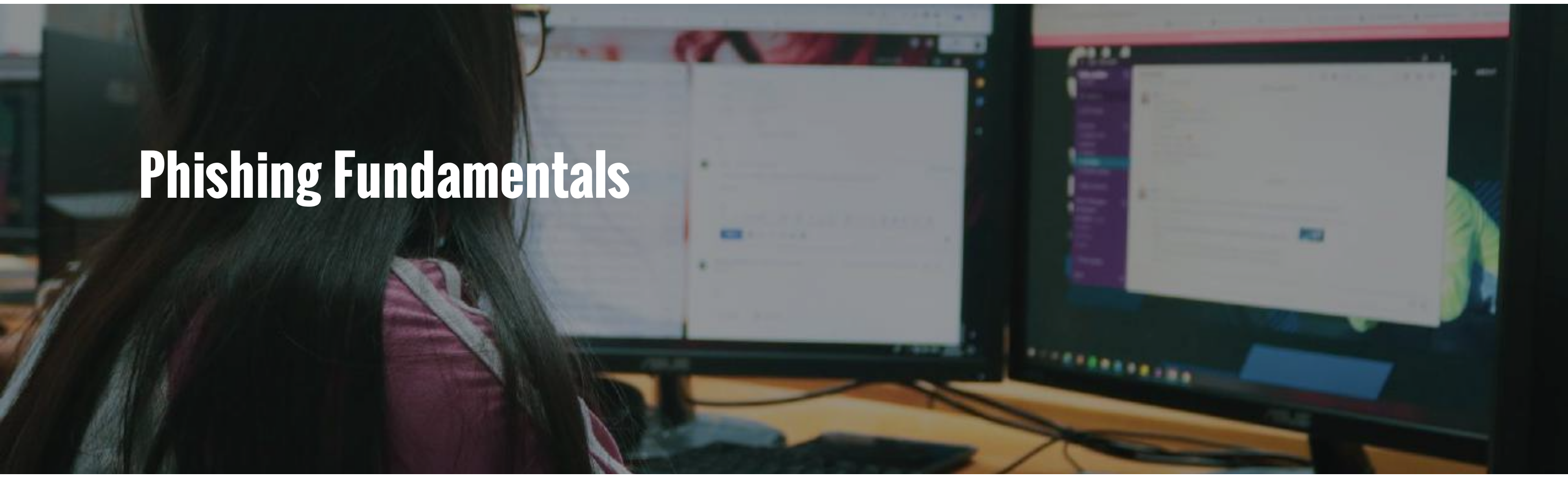


Phishing Fundamentals

VIGITRUST

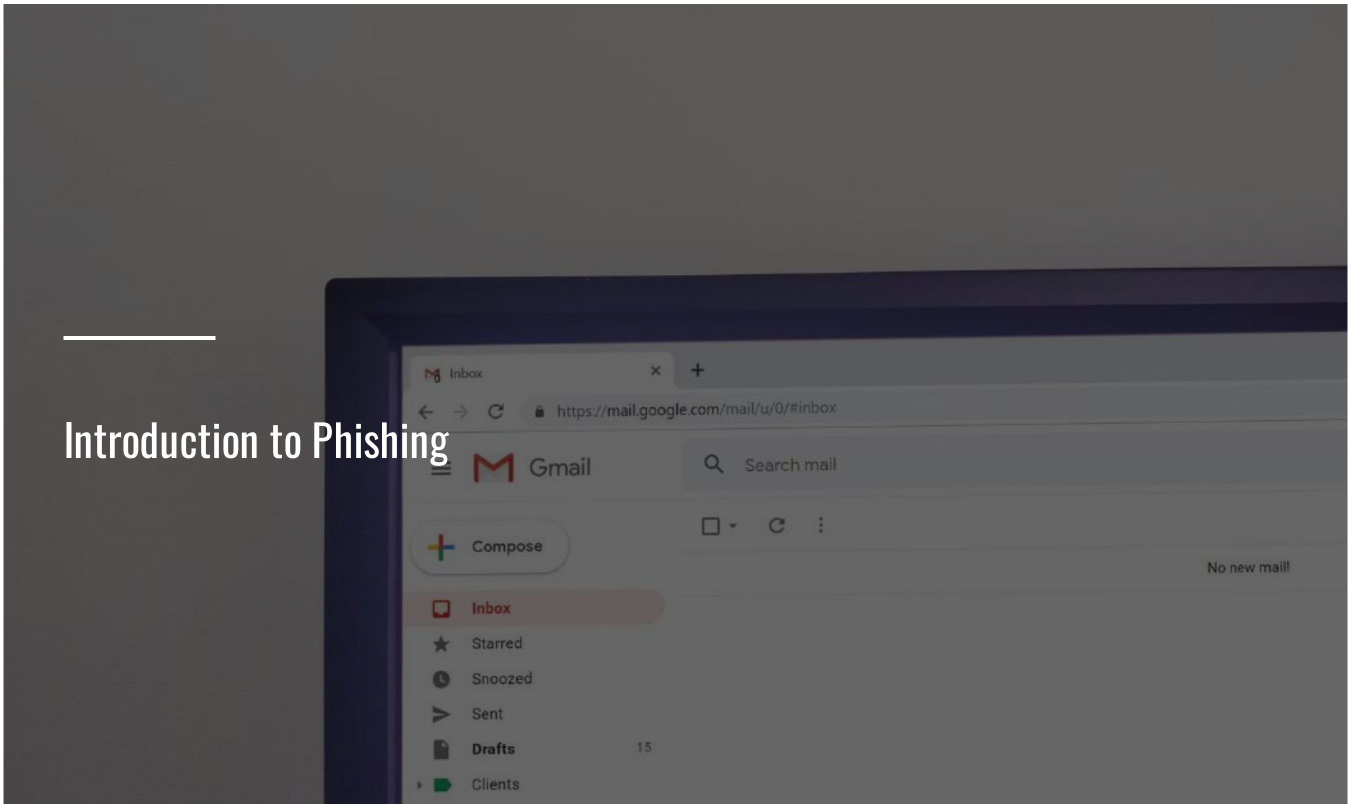
Phishing scams have been around for as long as the Internet itself, and continue to pose threat to the security of individuals and organizations. According to some statistics, phishing accounted for **90%** of all data breaches in 2019. Another study estimates that approximately **37%** of untrained users will fail to recognize phishing emails.
The aim of this course module is to provide with an understanding of phishing, how phishing scams work, and how to protect yourself and your company against them.

Click the Start Course button to begin!

Summary

Section 1 of 6

What Is Phishing?



Introduction to Phishing

Picture This

One day at work you receive an email from your "bank," informing you that there has been some "suspicious" activity on your account. The email instructs to to click on a link in order to "verify" your account details.

Click on the link below to "verify your account details "

Click here now!

Instead of directing you to a legitimate bank website, where you can "verify your account details", clicking on the link results in a particularly nasty form of malware being downloaded onto your computer. This malware will allow hackers to steal any personal information stored on the infected machine.

You've been phished!

What is Phishing?

Phishing is the fraudulent act of sending emails (or in some cases, text messages or phone calls) that purport to come from legitimate sources, such as banks and governmental organization in order to induce people to reveal information such a passwords, payment card details, or other sensitive information.

Phishing emails usually exhibit the following characteristics:

1. **Scammers pretend to be a reputable company or person you know.** Phishing emails commonly claim to come from your bank, the tax office, insurance companies or couriers, among many others. They may also appear to come from friends and colleagues, through email "spoofing".

2. **They ask you to click on a link, download an attachment, or provide sensitive information.** These actions may result in the infection of your computer with malware, ransomware or other nasty virus. Phishing emails will often direct targets to fake websites which look just like the real thing, where scammers collect the target's personal information.

3. **They use fear tactics or convey a sense of urgency.** Scammers commonly use phrases such as "suspicious activity on your account", "security incident" , or "update your password now" in order to encourage targets to take immediate action.

Another point about phishers is that they are **VERY** good at what they do. Phishing scams have become increasingly sophisticated in recent years - it is sometimes difficult, even for IT professionals, to distinguish the **real** from the **fake**.

In a phishing attack, scammers "bait" victims to click on a malicious link—or provide personal account or password information.

What Happens If You Get Hooked?

Your computer is infected with malware

Your computer is infected with ransomware

Your password is compromised

The scammers steal your credit card details

Sensitive company data is stolen

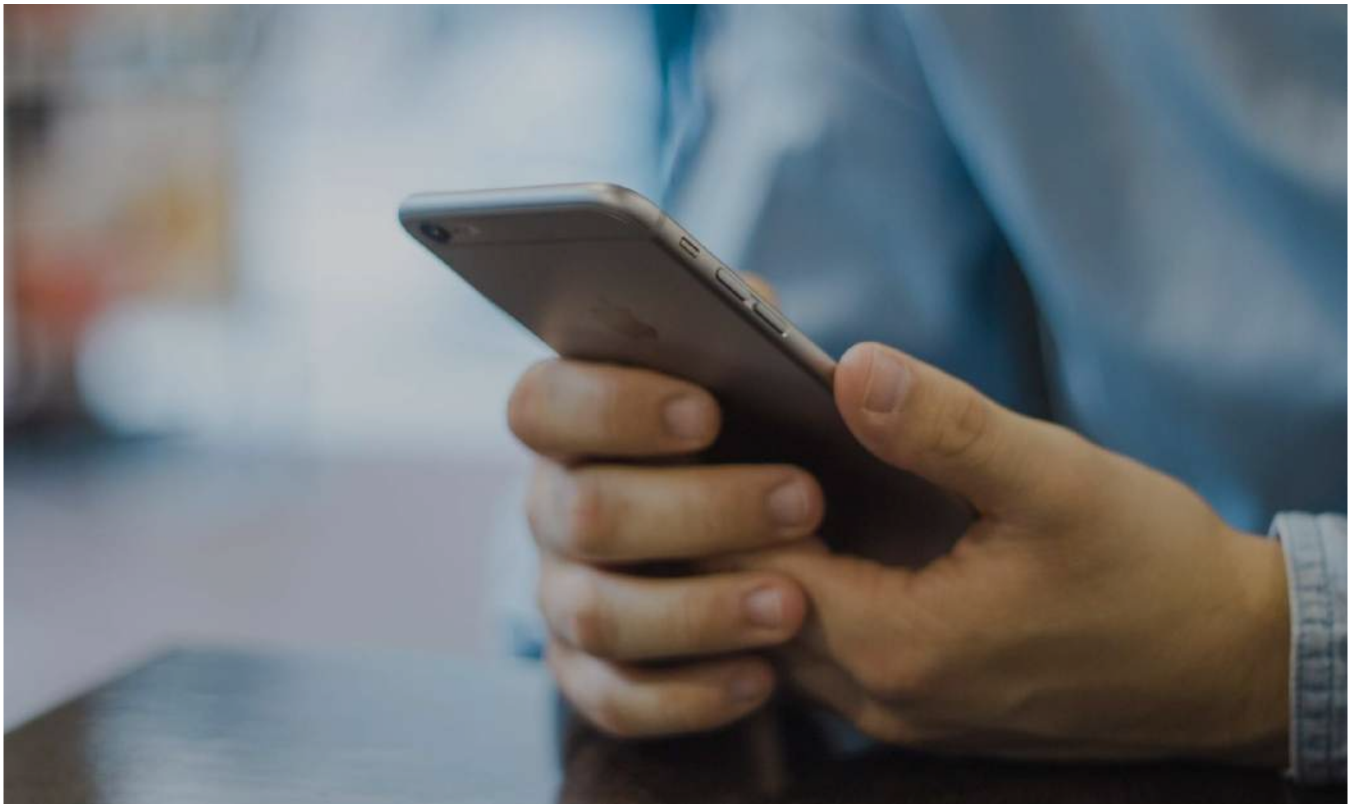
Your personal data is stolen

In the next lesson, you'll review some more specific examples of phishing scams and their sources.

CONTINUE

Section 2 of 6

Phishing Fundamentals



Phishing scams are often difficult to spot because they may appear to come from legitimate organizations, familiar brands, or other reputable sources.

What do Phishing Scams Look Like?

Phishing scams come in a wide variety of shapes and sizes, but most will exhibit one or more of the characteristics below:

- Claim that there's a problem with your account or password
- Ask you to confirm your password or account information
- Say that there's been suspicious activity on your account
- Ask you to click on a link or provide information for a new security update
- Offer you a free coupon, gift, or say that you're eligible for a refund
- Notify you of a failed or missed payment
- Attach a fake invoice

How do Phishers Target You?

Do you know the correct answer? Select which medium(s) phishers might use to target you. *Please select all responses that apply.*

□ Email

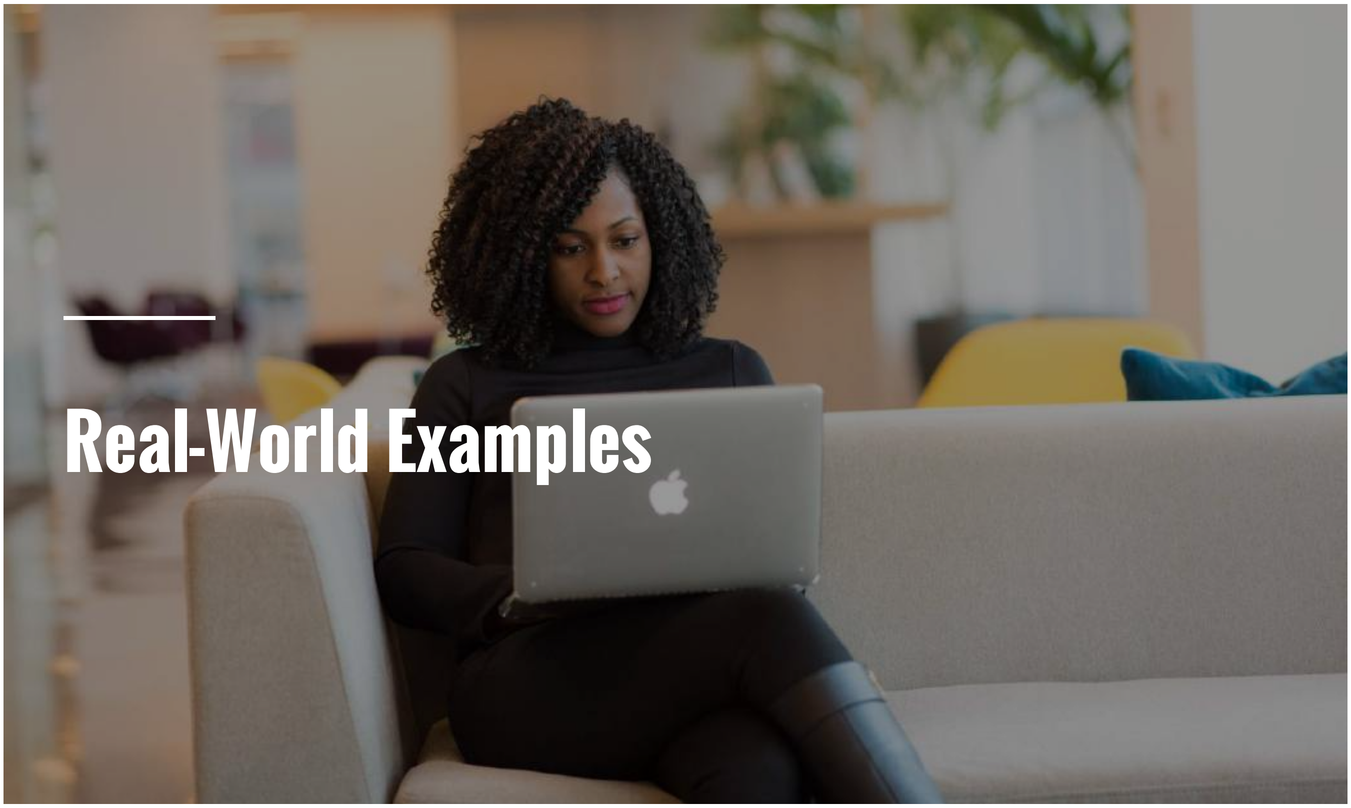
□ Text

□ Phone Call

SUBMIT

🔒 Complete the content above before moving on.

Phishing attacks can take place over email, text message, or over the phone. Anyone can be targeted—from contractors and full-time employees to company leaders.



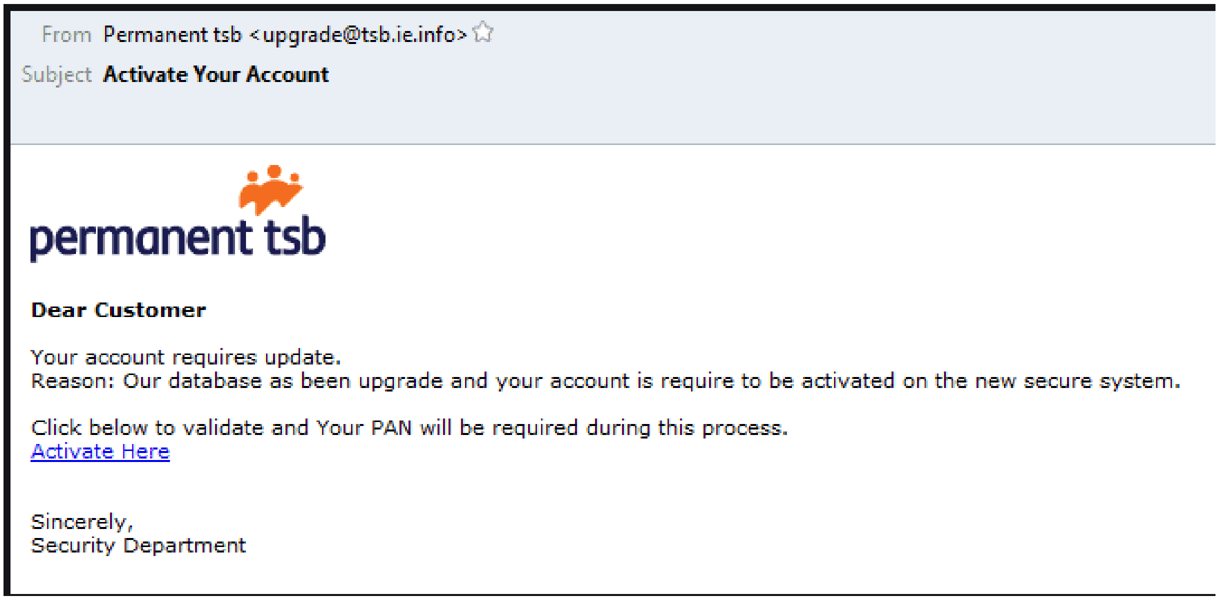
Real-World Examples

Expand Each Row Below

Here are some examples of phishing scams detected in recent years. We have included 3 types, each one representing a typical flavor.

Example One: We need to update your account

In this case the scammers attempt to persuade the target to update their account details via a link. Note the bad grammar and generic salutations ('dear customer'). This is fairly typical of phishing emails (more on this later).



From Permanent tsb <upgrade@tsb.ie.info>

Subject **Activate Your Account**

permanent tsb

Dear Customer

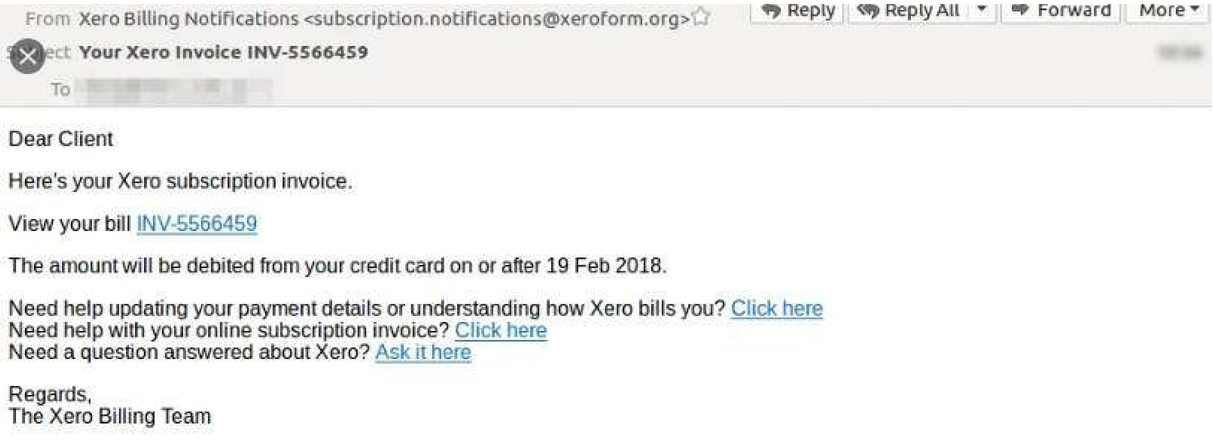
Your account requires update.
Reason: Our database as been upgrade and your account is require to be activated on the new secure system.

Click below to validate and Your PAN will be required during this process.
Activate Here

Sincerely,
Security Department

Example Two: Fake Invoice

Sometimes scammers will target individuals with fake invoices. The "invoice" may take the form of an email attachment, or a link may be provided in the email body.



From Xero Billing Notifications <subscription.notifications@xeroform.org>

ect Your Xero Invoice INV-5566459 [redacted]

To [redacted]

Dear Client

Here's your Xero subscription invoice.

View your bill INV-5566459

The amount will be debited from your credit card on or after 19 Feb 2018.

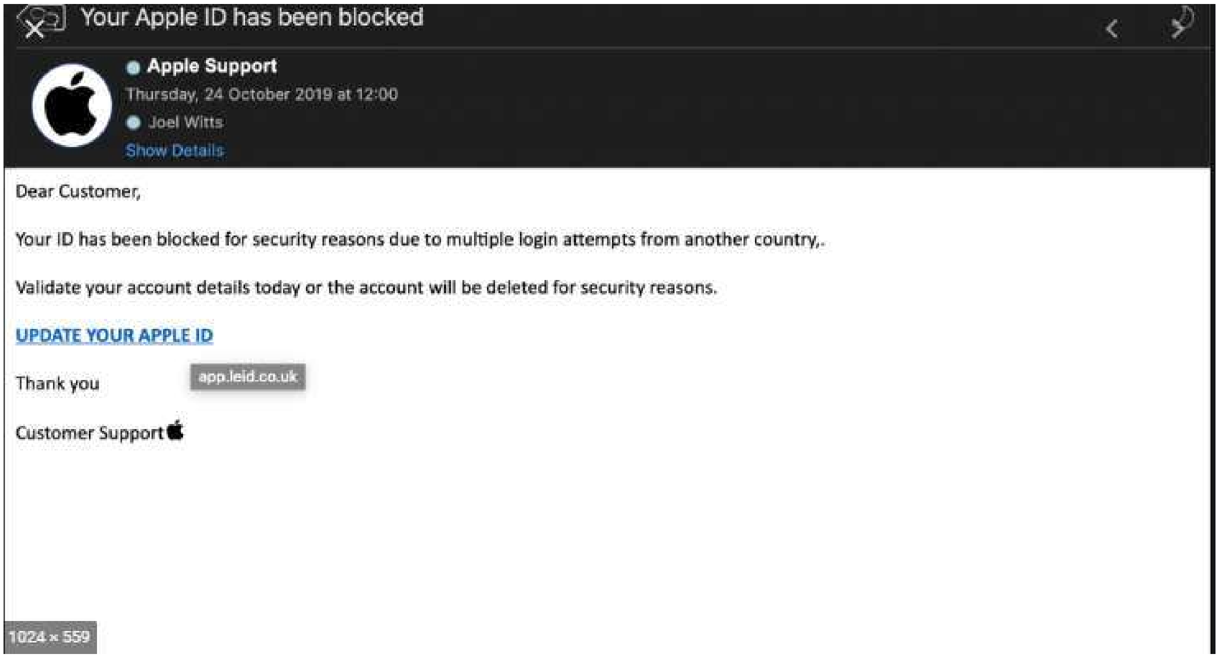
Need help updating your payment details or understanding how Xero bills you? Click here
Need help with your online subscription invoice? Click here
Need a question answered about Xero? Ask it here

Regards,
The Xero Billing Team

Example Three: There has been a security breach

—

This example displays the classic phishing tactic of attempting to instill a sense of fear into the target (' multiple logins from another country').



Your Apple ID has been blocked

Apple Support
Thursday, 24 October 2019 at 12:00
Joel Witts
Show Details

Dear Customer,

Your ID has been blocked for security reasons due to multiple login attempts from another country,.

Validate your account details today or the account will be deleted for security reasons.

UPDATE YOUR APPLE ID

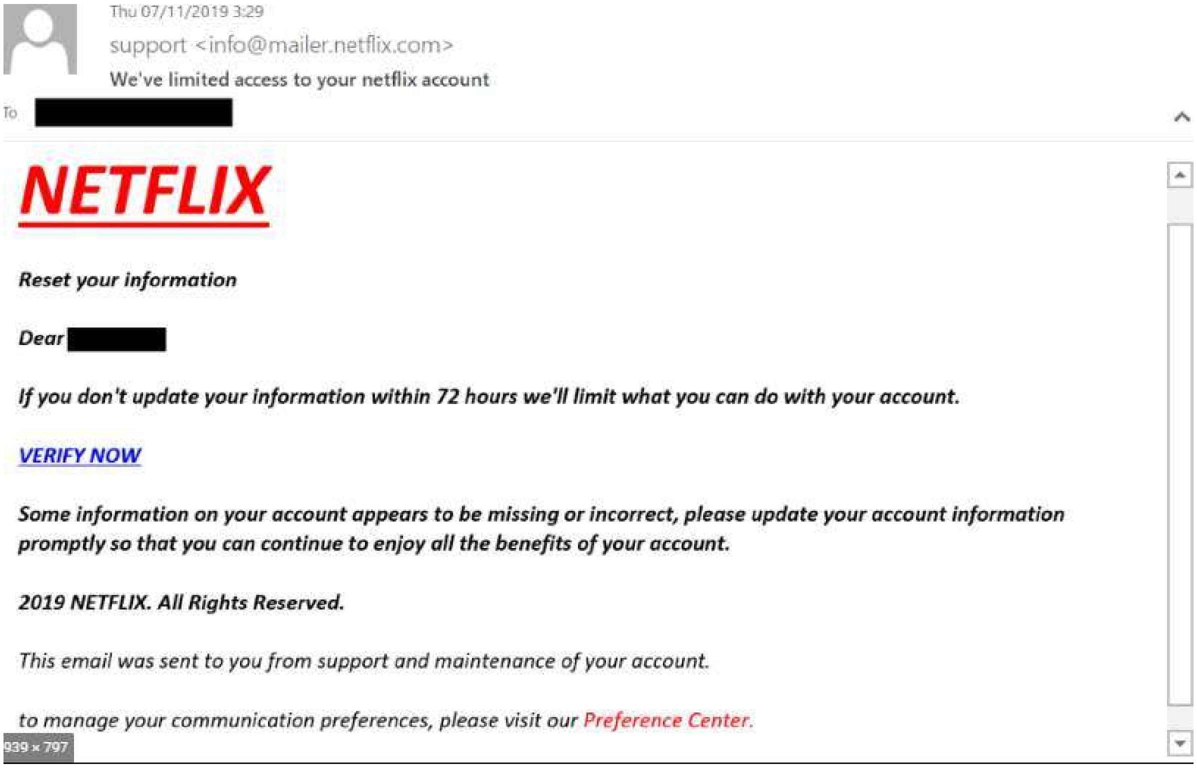
Thank you

Customer Support

Example Four: Spear Phishing

—

This is an example of more insidious form of phishing, so-called spear phishing. These emails tend to be targeted at specific groups, for example employees at the same organization or, as in this case, a well-known brand's customer base. Spear phishing emails tend to be more convincing, and therefore more dangerous.



Thu 07/11/2019 3:29

support <info@mailer.netflix.com>

We've limited access to your netflix account

To [redacted]

NETFLIX

Reset your information

Dear [redacted]

If you don't update your information within 72 hours we'll limit what you can do with your account.

VERIFY NOW

Some information on your account appears to be missing or incorrect, please update your account information promptly so that you can continue to enjoy all the benefits of your account.

2019 NETFLIX. All Rights Reserved.

This email was sent to you from support and maintenance of your account.

to manage your communication preferences, please visit our Preference Center.

In the next lesson, you'll learn what specific signs to look for to be able to flag and avoid phishing attempts successfully.

Identify: How to Spot Phishing Attempts

Phishing Attempts Can Be Tricky to Spot

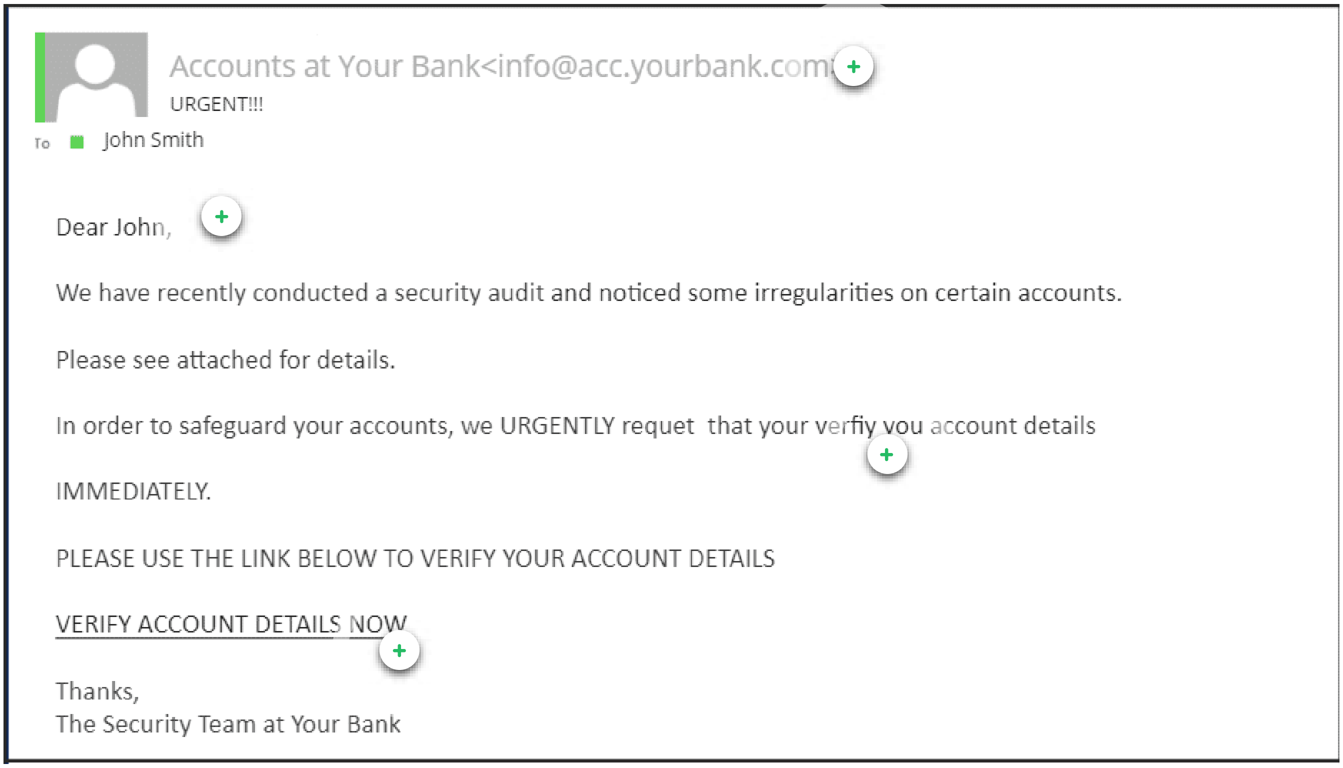
As you have already seen, phishing scams are becoming increasingly sophisticated and harder to detect. Phishers can easily unearth information about you on company websites, social media sites and any other public profiles available online. The upshot of this is that they can tailor communications towards you - and make scams harder to detect.

.

> Phishers can easily unearth information about you on company websites, social media sites and any other public profiles available online.

Look for the Classic Signs

The graphic (below) is based on numerous examples of real phishing emails and points out red flags that give the scam away. Click on each marker to see some examples of "red flags" that should arouse your suspicion!



Accounts at Your Bank<info@acc.yourbank.com>

URGENT!!!

To John Smith

Dear John,

We have recently conducted a security audit and noticed some irregularities on certain accounts.

Please see attached for details.

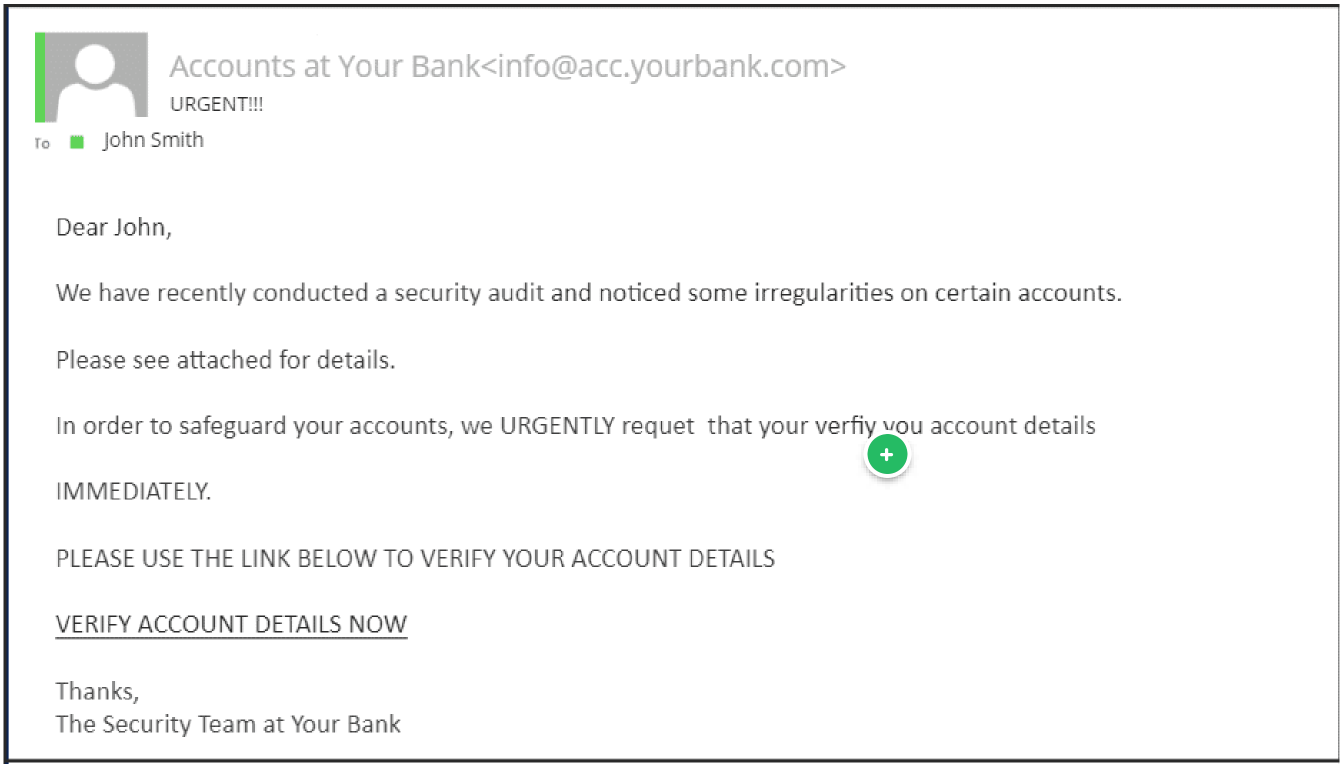
In order to safeguard your accounts, we URGENTLY requet that your verfiy you account details

IMMEDIATELY.

PLEASE USE THE LINK BELOW TO VERIFY YOUR ACCOUNT DETAILS

VERIFY ACCOUNT DETAILS NOW

Thanks,
The Security Team at Your Bank



Accounts at Your Bank<info@acc.yourbank.com>

URGENT!!!

To John Smith

Dear John,

We have recently conducted a security audit and noticed some irregularities on certain accounts.

Please see attached for details.

In order to safeguard your accounts, we URGENTLY requet that your verfiy you account details

IMMEDIATELY.

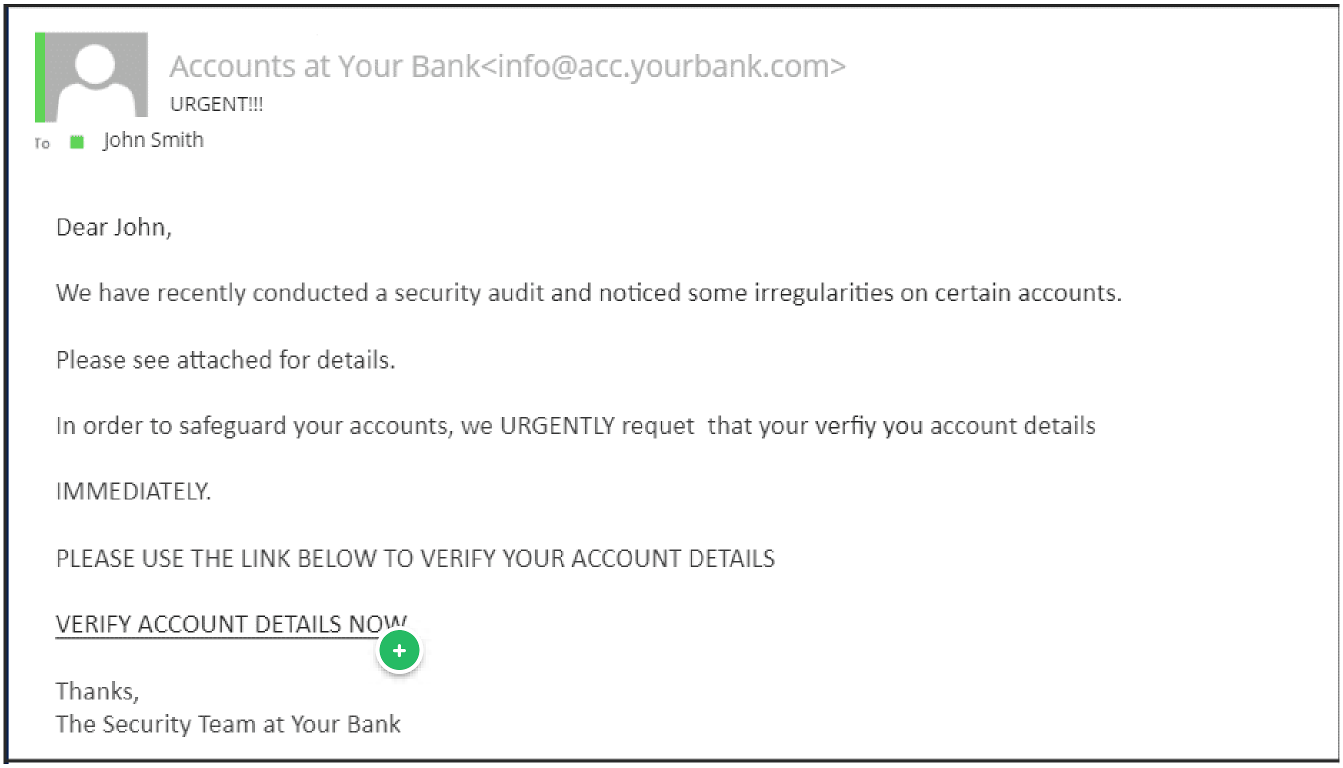
PLEASE USE THE LINK BELOW TO VERIFY YOUR ACCOUNT DETAILS

VERIFY ACCOUNT DETAILS NOW

Thanks,
The Security Team at Your Bank

Grammar, Spelling, or Punctuation Errors

Phishing emails often contain poor grammar, spelling or punctuation (although not always!). Ask yourself - would my bank/insurer/ISP send me an email full of spelling mistakes?



Accounts at Your Bank<info@acc.yourbank.com>

URGENT!!!

To John Smith

Dear John,

We have recently conducted a security audit and noticed some irregularities on certain accounts.

Please see attached for details.

In order to safeguard your accounts, we URGENTLY requet that your verfiy you account details

IMMEDIATELY.

PLEASE USE THE LINK BELOW TO VERIFY YOUR ACCOUNT DETAILS

VERIFY ACCOUNT DETAILS NOW

Thanks,
The Security Team at Your Bank

Hyperlinks or Attachments

Phishing emails often contain instructions that encourage recipients to, for example, update their account/password/ payment card details via a link included in the message.
These links may direct users to fake or malicious websites, where users are encouraged to enter personal details or download ‘free’ software (i.e. malware).
Legitimate organizations would never request information in this way.
To test, hover your mouse over the link. If the link looks strange or unfamiliar it is most likely a phishing scam.

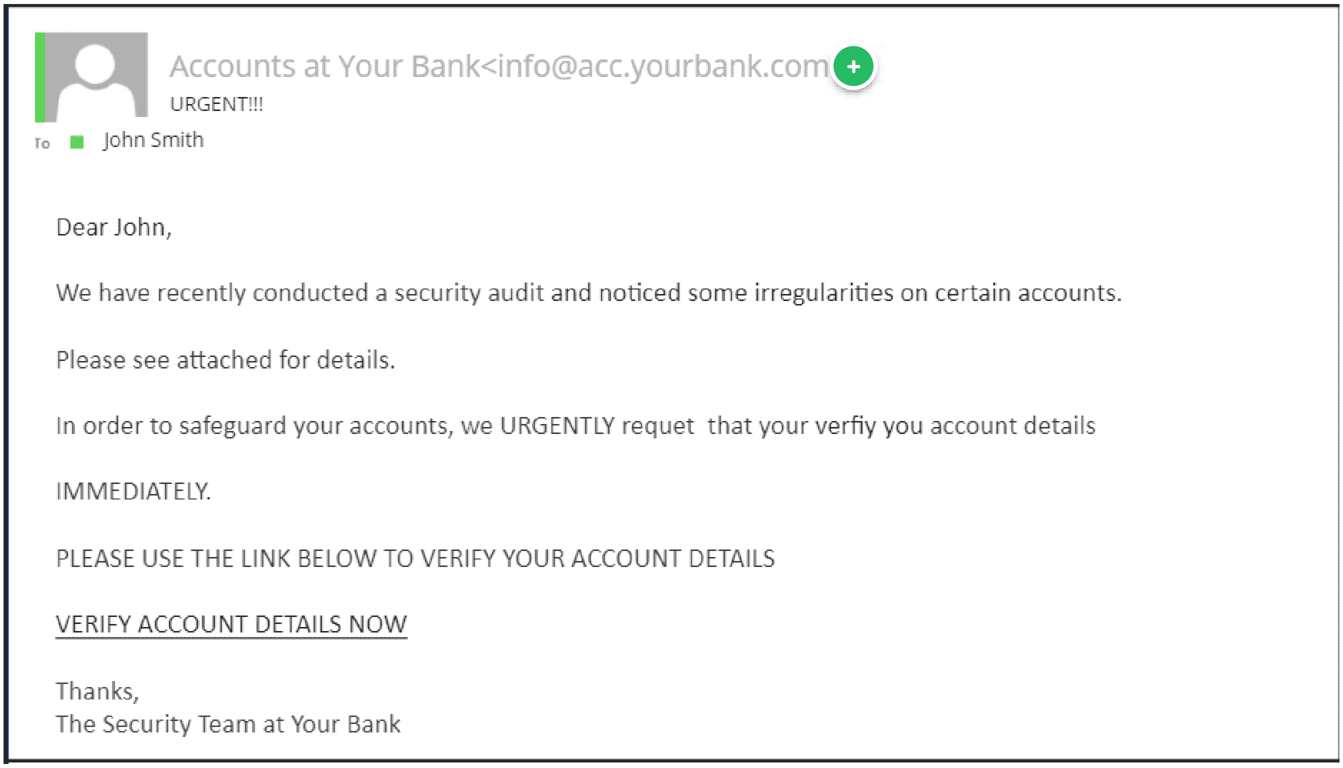
Here's a few things to look out for:

- Links that don't match the destination
- Links with misspellings
- Links with little context or explanation

Attachments.
Phishing emails often include attachments purporting to be forms, invoices, etc. NEVER click on these - they may contain viruses.
Look out for:

- Unexpected attachments

- Attachments ending in .exe



Accounts at Your Bank<info@acc.yourbank.com

URGENT!!!

To John Smith

Dear John,

We have recently conducted a security audit and noticed some irregularities on certain accounts.

Please see attached for details.

In order to safeguard your accounts, we URGENTLY requet that your verfiy you account details

IMMEDIATELY.

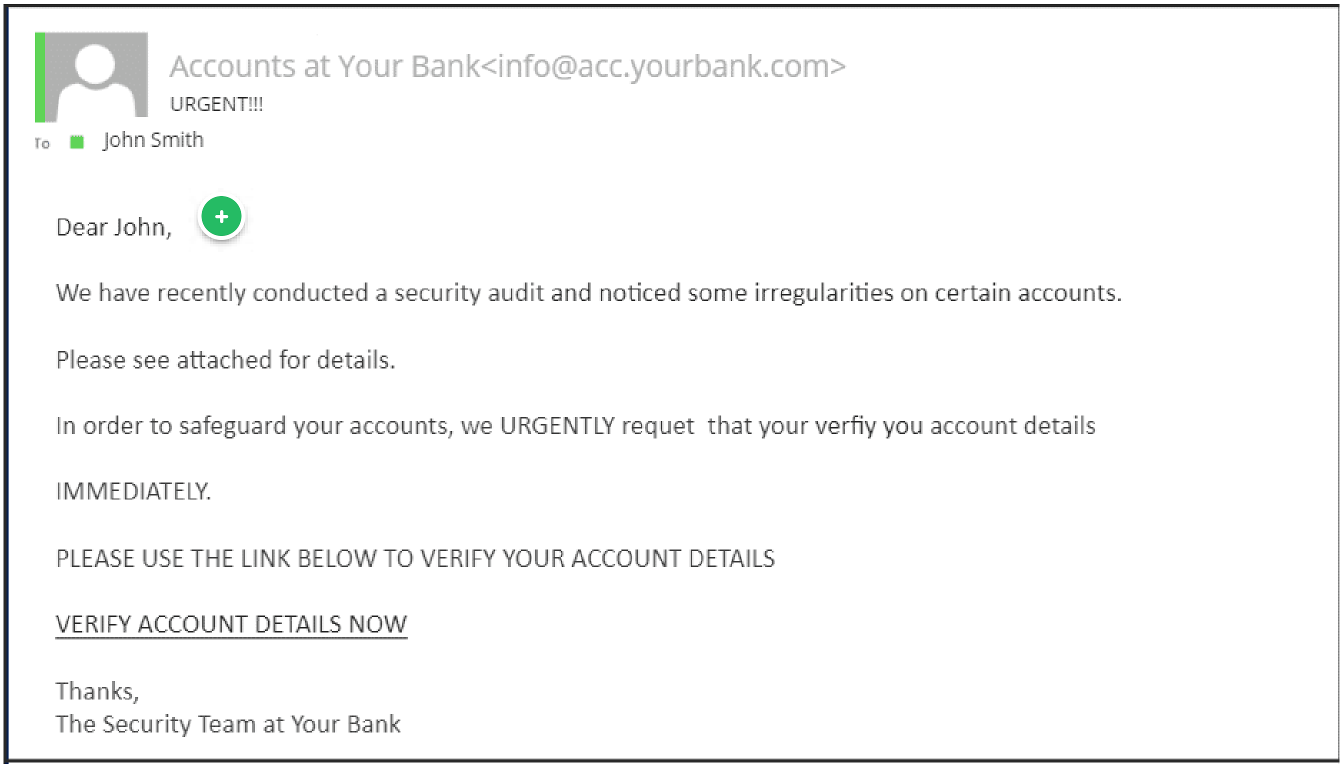
PLEASE USE THE LINK BELOW TO VERIFY YOUR ACCOUNT DETAILS

VERIFY ACCOUNT DETAILS NOW

Thanks,
The Security Team at Your Bank

Unfamiliar or Illegitimate Senders

Check the sender's email address. Is it legitimate? Does it match the standard address for the company that the email claims to represent?



Accounts at Your Bank<info@acc.yourbank.com>
URGENT!!!
To John Smith

Dear John,

We have recently conducted a security audit and noticed some irregularities on certain accounts.

Please see attached for details.

In order to safeguard your accounts, we URGENTLY requet that your verfiy you account details

IMMEDIATELY.

PLEASE USE THE LINK BELOW TO VERIFY YOUR ACCOUNT DETAILS

VERIFY ACCOUNT DETAILS NOW

Thanks,
The Security Team at Your Bank

Subject Line or Salutation

Subject lines. Phishing emails tend to use attention-grabbing subject lines so as to arouse the curiosity of the target. For example, "Urgent" or "Suspicious Activity on Your Account" .

Salutations. Phishing emails often use generic salutations such as:

- Dear Valued Customer
- Dear Member
- Dear Customer
- Dear Sir/Madam
- Dear User
- Hi There

However, as we have seen, phishers are increasingly adept at personalizing messages, so it common for phishing emails to include the name of the target.

Additional Questions to Ask Yourself

If you receive an email that you feel is suspicious, ask yourself:

Is the email unsolicited?

Did this message just arrive out of the blue?

1 of 5

Does it ask for your personal or account information?

A classic sign - ALWAYS remember that a legitimate organization such as a bank or tech company would NEVER request that you provide personal or confidential information via email.

2 of 5

Does it use fear tactics?

Again, a classic phishing tactic to encourage you to take action.

3 of 5

Does it offer you something for free?

Emails that purport to offer you 'free' stuff should always arouse your suspicion.

4 of 5

Does the email feel strange or does it not make sense?

If it looks and feels like phishing, then it most likely is phishing!

5 of 5

A Final Checklist

Some things to remember:

□ **Beware of unsolicited emails.** Be suspicious of emails containing links or attachments from people you don't know.

□ **Examine who sent the message—and who else received it.** Carefully examine the email header and check with your colleagues to see if they received something similar.

□ **Flag generic subject lines and salutations.** Such as "Dear Sir/Madam", "Dear Customer".

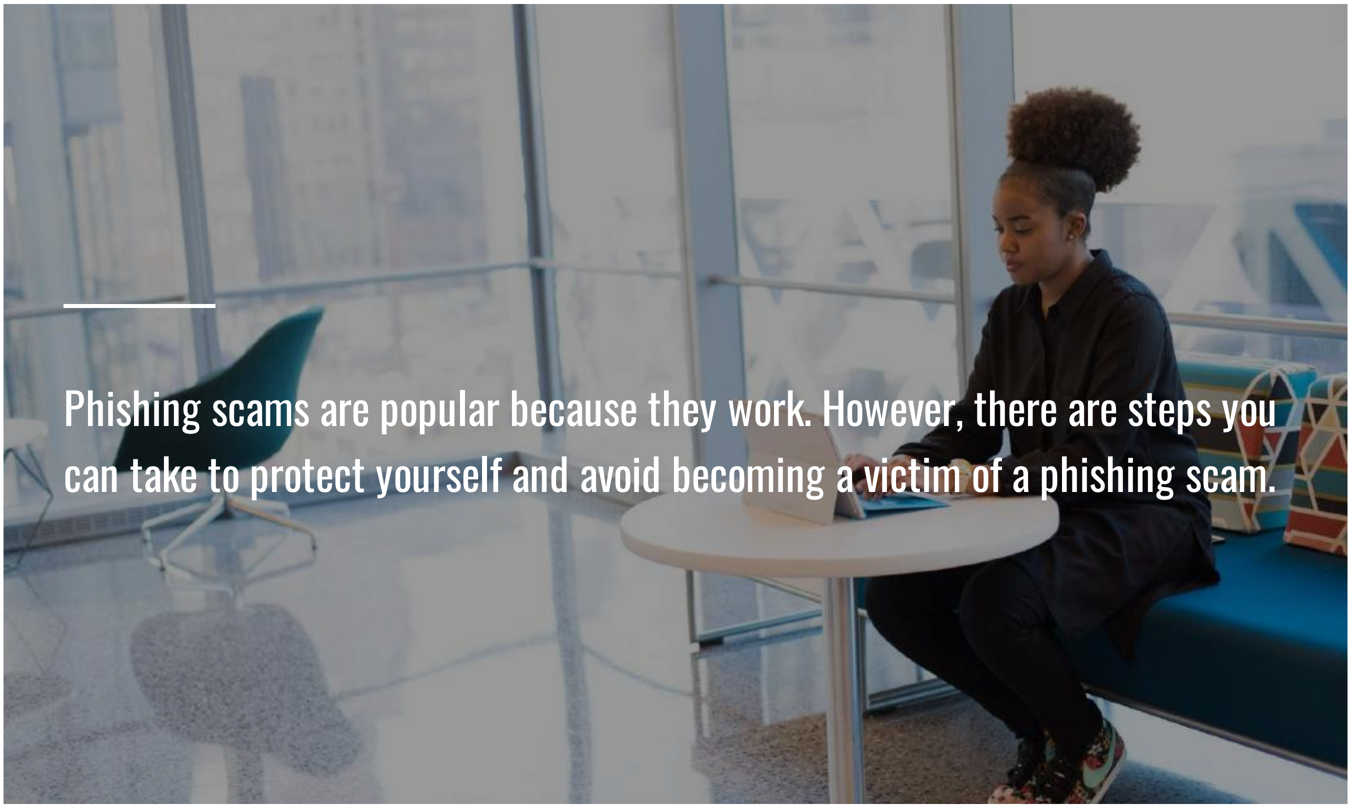
□ **Be suspicious of hyperlinks or attachments.** This is the phisher's objective - to get you to click on a link or download an attachment.

□ **Check for spelling, grammar, or punctuation errors.** Legitimate organizations would never send you an email containing typos!

Delete the email if you notice any of these signs. NEVER click on the email's links or attachments. Better still—don't even *open* the email if it feels suspicious. In the next lesson, you'll learn what else you can do to protect yourself and avoid phishing scams.

Section 4 of 6

Steps to Protect Yourself from Phishing Attacks



Phishing scams are popular because they work. However, there are steps you can take to protect yourself and avoid becoming a victim of a phishing scam.

Enhance Security with the Right Systems and Tools

Here are some tips to protect yourself, and your organization, from phishing attacks:

Set Up Multi-Factor Authentication

Multi-factor authentication can help protect systems from attacks by phishers and hackers using phished credentials.

Turn on Spam Filters and Browser Extensions

Spam filters can detect and block phishing emails before they reach your inbox. In addition there are many browser extensions available (both free and paid) that can help to detect and flag phishing sites.

Use Firewalls and Antivirus Software

Always make sure your computer's firewall is functioning correctly - never attempt to switch it off! Anti-virus software should be up-to-date and running at all times.

Do's and Don'ts to Protect Yourself

Drag and drop the following 'Do's and 'Don'ts' of phishing to the correct location:

Do

Beware of unsolicited emails

Be suspicious of unsolicited emails containing links or attachments

Delete suspicious emails - don't open them

Inform your manager or IT department if you receive a suspicious email

Remember if it looks like phishing, it probably is phishing"

Don't

Click on links or download attachments in unsolicited emails

Switch off your computer's firewall or anti-virus software

Share personal information on social media sites

Provide personal information to suspicious websites

Summary

Phishing represents an ever present threat to the security of information to you and your company.

- **Remember, if an email looks like phishing, it probably is phishing!**
- **Never click on links or download attachments in emails from people you don't know.**

Section 5 of 6

Respond: What to Do If You Think You've Been Phished

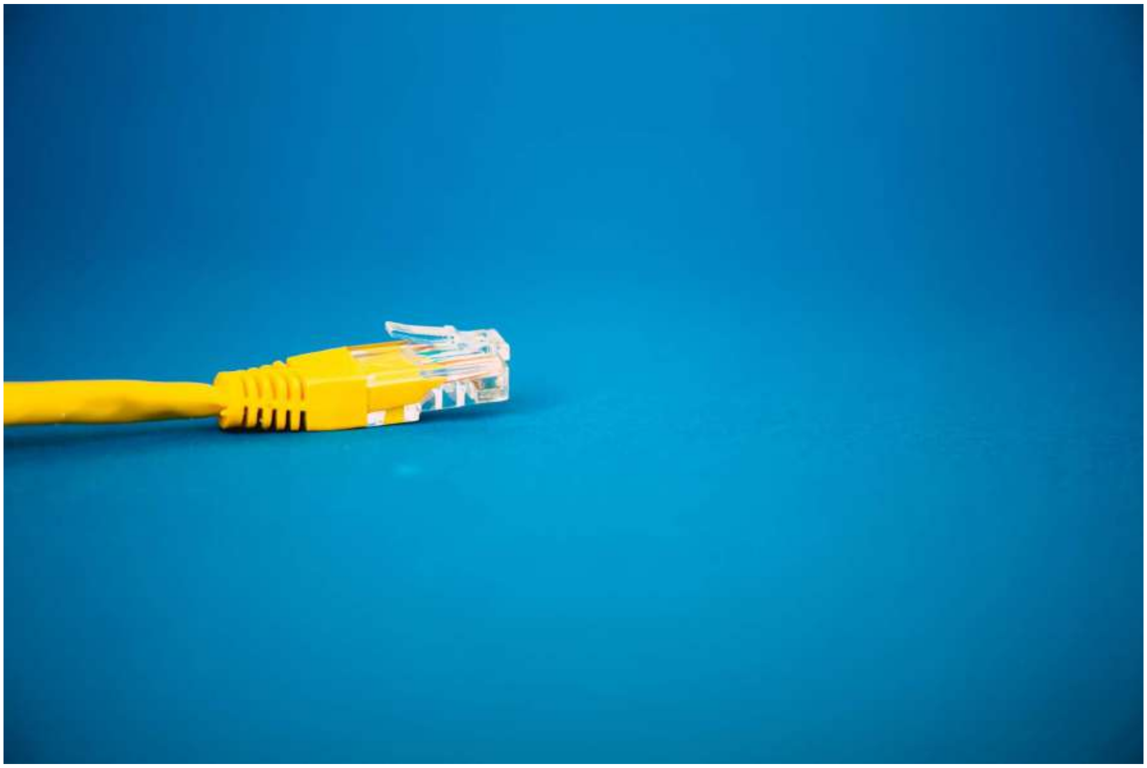
You've be Phished. Now What?

Should you be unlucky enough to be the victim of a phishing scam, we suggest you follow these steps:

Five Steps to Minimize the Damage

Step 1

Go Offline



If working at home, disconnect your computer from the Internet to prevent your data being stolen. If at work, disconnect your computer from the local area network to prevent the spread of any virus and protect your data.

Step 2

Back Up Your Files

Is is always sensible to maintain a backup of all your files and folders. This is particularly important in the case of a ransomware attack, where scammers encrypt files and demand payment in return for decrypting them.

Step 3

Report It

Report the incident to your manager or IT department immediately!

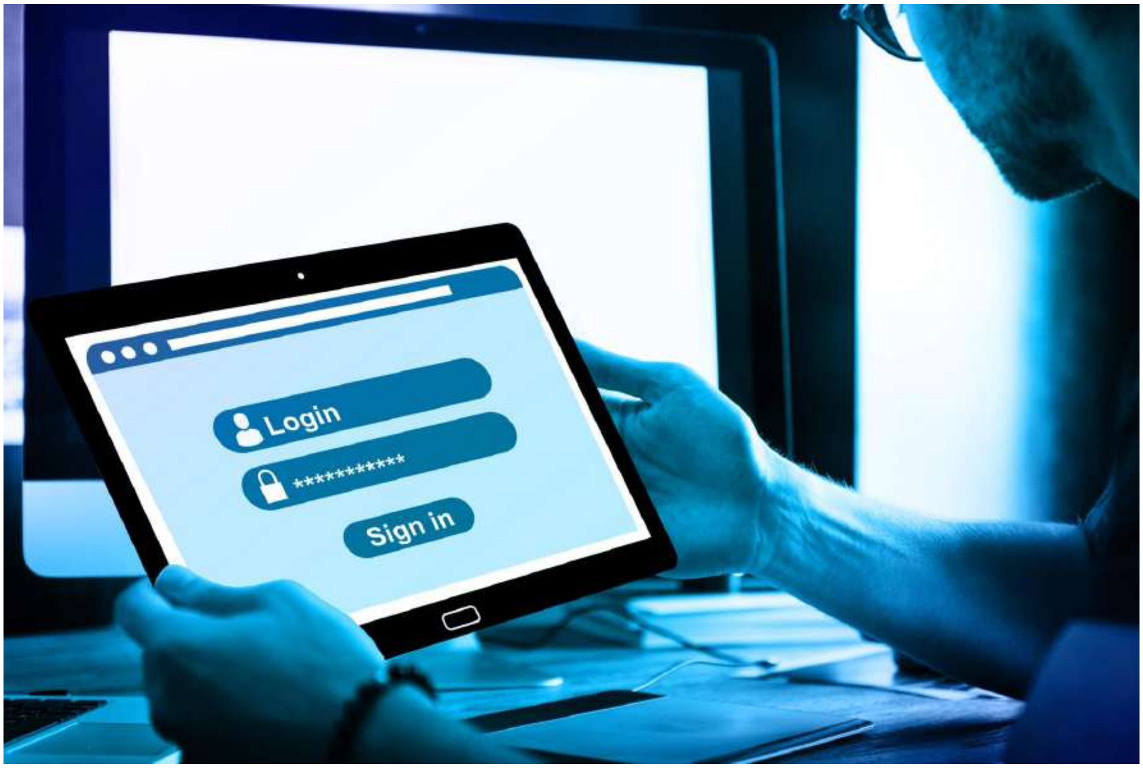
Step 4

Scan Your System for Malware

Perform a complete system scan if you believe your computer has been compromised by malware.

Step 5

Change Your Passwords



Change your password/s **immediately** to prevent systems being compromised.

Summary

Following these steps should help reduce the impact of a phishing attack. However, the key is to prevent such incidents in the first place. Prevention is better than cure!

Reporting a Security Incident

ⓘ **If you believe you have been the victim of a phishing scam, or receive a suspicious email, text message or phone call, contact your IT department immediately!**

Section 6 of 6

Summary

And finally...

Key Takeaways

1. Phishing is the fraudulent act of sending emails (or in some cases, text messages or phone calls) that purport to come from legitimate sources, such as banks and governmental organization in order to induce people to reveal information such a passwords, payment card details, or other sensitive information.

2. **Phishing scams have become increasingly sophisticated and hard to detect. Things to look out for include links and attachments in unsolicited emails, bad**

spelling and grammar, generic recipient names and language designed to induce a sense of urgency among recipients.

3 Protect yourself from phishing scams by exercising common sense - never click on links or attachments in emails from unknown senders. **THINK** before opening an email or attachment.

4 **If you do fall victim to a phishing scam, disconnect from the Internet or network, scan your computer for viruses, backup your files and notify your IT department of manager immediately.**

Consider This: What Would a Legitimate Organization Do?

Finally, a quick summary contrasting the actions of legitimate organizations and phishing scammers. Click on each card to learn more.

Legitimate Organizations

- Use secure and encrypted websites
- Have standard email addresses and logos
- Don't request personal information by email

- Use fear tactics

Phishers

- Ask you to share your password or other personal information
- Attempt to induce you to click on links and download

Thank you for completing this course!