Contents

Here at Virtual Assist USA, security is one of our top priorities. As technology advances there is going to be a rise of spam, phishing emails, malware and other security risks. This document will assist in different ways to protect you and your business against these rising risks!

Phishing is one of the most common methods of cyber-crime, but despite how much we think we know about scam emails, people still frequently fall victim. We don’t want that for you.

Email Security

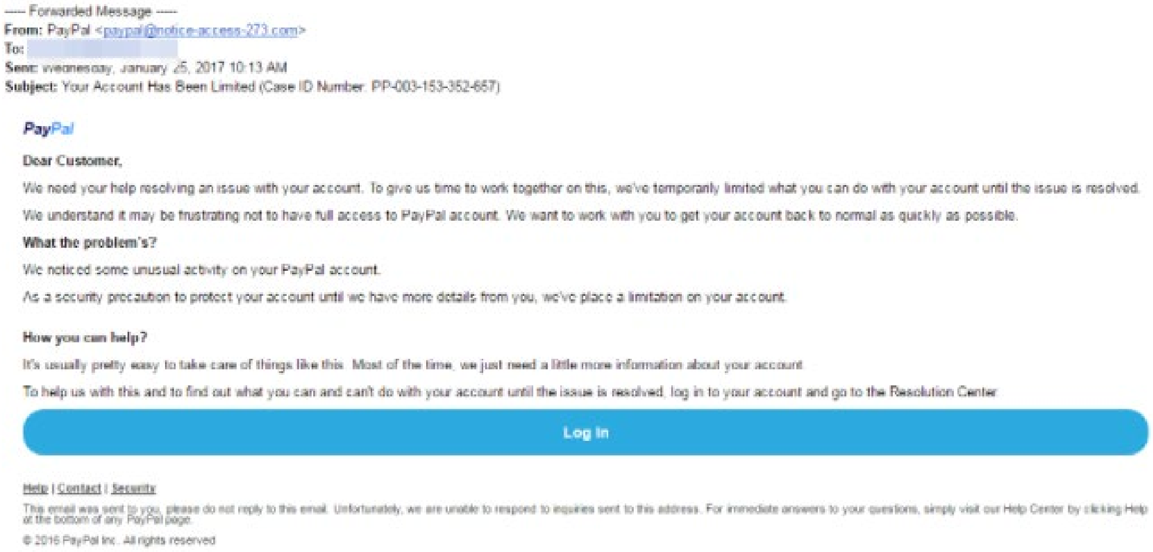
Here are some things that we at Virtual Assist USA urge you and your employees to look for when receiving an email from someone new:

The message is sent from a public email domain.

Examples of this are:

- Legitimate organizations will not send emails from an address that ends ‘@gmail.com’.
- Not even Google.
- Many organizations with the exception of some small operations, will have their own email domain and company accounts. For example, legitimate emails from Google will read ‘@google.com’.
- If the domain name (the bit after the @ symbol) matches the apparent sender of the email, the message is most likely legitimate.
- The best way to check an organization’s domain name is to type the company’s name into a search engine.
- This makes detecting phishing seem easy, but cyber criminals have plenty of tricks up their sleeves to deceive you.

Tip: Look at the email address, not just the sender



----- Forwarded Message -----
From: PayPal <paypal@notice-access-273.com>
To: [redacted]
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

This is a nearly flawless scam email. It uses PayPal’s logo at the top of the message, it is styled professionally and the request is believable.

But as much as it attempts to replicate a genuine email from PayPal, there’s one huge red flag: the sender’s address is ‘paypal@notice-access-273.com’. This should put you on high alert.

The domain name is misspelled.

There’s another clue hidden in domain names that provide a strong indication of phishing scams – and it unfortunately complicates our previous clue.

The problem is that anyone can buy a domain name from a registrar. And although every domain name must be unique, there are plenty of ways to create addresses that are indistinguishable from the one that’s being spoofed.

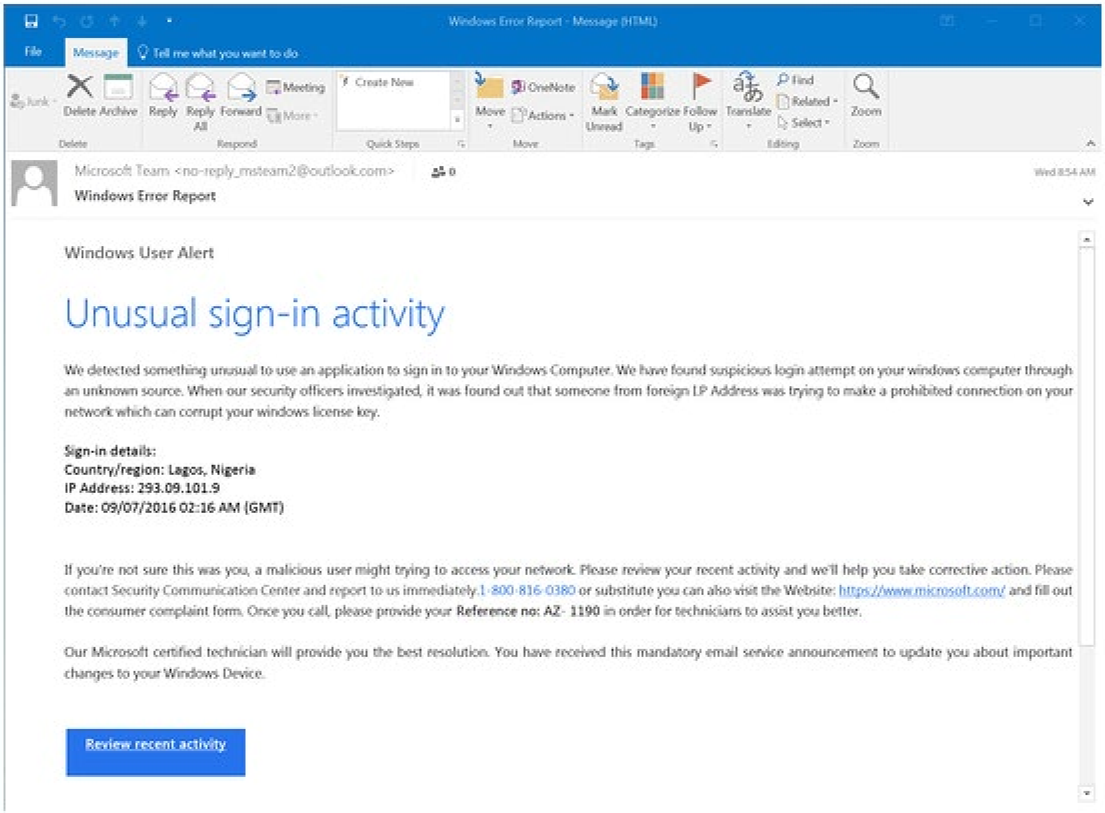
The email is poorly written.

You can often tell if an email is a scam if it contains poor spelling and grammar.

Many people will tell you that such errors are part of a ‘filtering system’ in which cyber criminals target certain people.

The theory is that, if someone ignores clues about the way the message is written, they're less likely to pick up clues during the scammer's endgame.

Tip: Look for grammatical mistakes, not just spelling mistakes



Microsoft Team <no-reply_msteam2@outlook.com>

Windows Error Report

Windows User Alert

Unusual sign-in activity

We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign I.P Address was trying to make a prohibited connection on your network which can corrupt your windows license key.

Sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 09/07/2016 02:16 AM (GMT)

If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your **Reference no: AZ- 1190** in order for technicians to assist you better.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

Review recent activity

Look at the context of the error and determine whether it's a clue to something more sinister. You can do this by asking a few questions:

- Is it a common sign of a typo (like hitting an adjacent key)?
- Is it a mistake a native speaker shouldn't make (grammatical incoherence, words used in the wrong context)?
- Is this email a template, which should have been crafted and copy-edited?
- Is it consistent with previous messages I've received from this person?

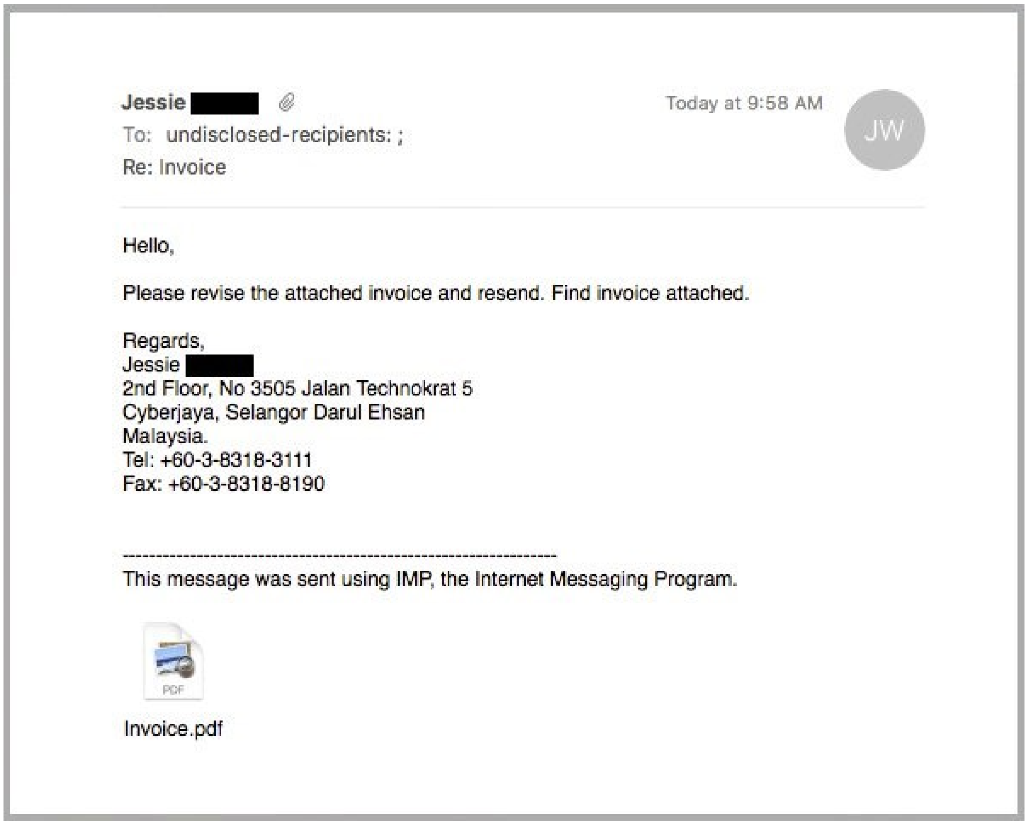
If you're in any doubt, look for other clues that we've listed here or contact the sender using another line of communication, whether that's in person, by phone, via their website, an alternative email address or through an instant message application.

It includes suspicious attachments or links

Phishing emails can come in many different forms including social media posts and text messages. But no matter how phishing emails are delivered, they all contain a payload. This will either be an infected attachment that you're asked to download or a link to a website that is not legitimate.

The purpose of these payloads is to capture sensitive information, such as your login credentials, credit card details, phone numbers and account numbers.

An infected attachment is a seemingly benign document that contains malware. In a typical example, like the one below, the phisher claims to be sending an invoice:



Jessie [redacted]

Today at 9:58 AM

To: undisclosed-recipients: ;

Re: Invoice

Hello,

Please revise the attached invoice and resend. Find invoice attached.

Regards,
Jessie [redacted]
2nd Floor, No 3505 Jalan Technokrat 5
Cyberjaya, Selangor Darul Ehsan
Malaysia.
Tel: +60-3-8318-3111
Fax: +60-3-8318-8190

This message was sent using IMP, the Internet Messaging Program.

Invoice.pdf

It doesn't matter whether you were expecting to receive an invoice from this person or not, because in most cases you won't be sure what the message pertains to until you open the attachment.

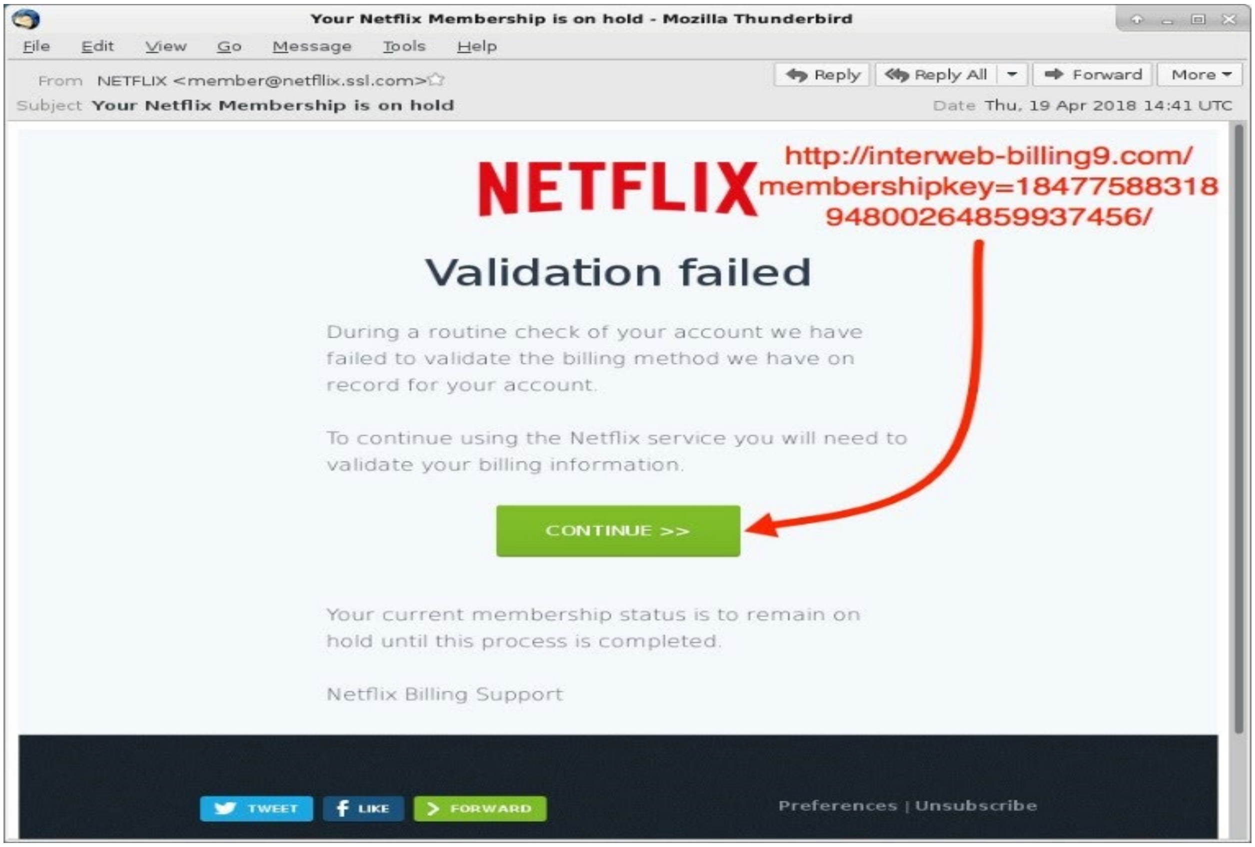
When you open the attachment, you'll see that the invoice isn't intended for you, but it will be too late. The document unleashes malware on your computer, which could perform any number of nefarious activities.

Suspicious links

You can spot a suspicious link if the destination address doesn't match the context of the rest of the email.

For example, if you receive an email from Netflix, you would expect the link to direct you towards an address that begins ‘netflix.com’.

Unfortunately, many legitimate and scam emails hide the destination address in a button, so it’s not immediately apparent where the link goes to.



From NETFLIX <member@netfllix.ssl.com>

Subject Your Netflix Membership is on hold

Date Thu, 19 Apr 2018 14:41 UTC

http://interweb-billing9.com/membershipkey=18477588318948002648599374 56/

Validation failed

During a routine check of your account we have failed to validate the billing method we have on record for your account.

To continue using the Netflix service you will need to validate your billing information.

Your current membership status is to remain on hold until this process is completed.

Netflix Billing Support

The message creates a sense of urgency

Scammers know that a lot of us procrastinate. We receive an email giving us important news, and we decide we’ll deal with it later. We’ve all done it.

But the longer you think about something, the more likely you are to notice things that don’t seem right.

Maybe you realize that the organization doesn’t contact you by that email address, or you speak to a colleague and learn that they didn’t send you a document.

Even if you don’t get that ‘aha!’ moment, coming back to the message with a fresh set of eyes might help reveal its true nature.

That's why so many scams request that you act now or else it will be too late. This has been evident in every example we've used so far.

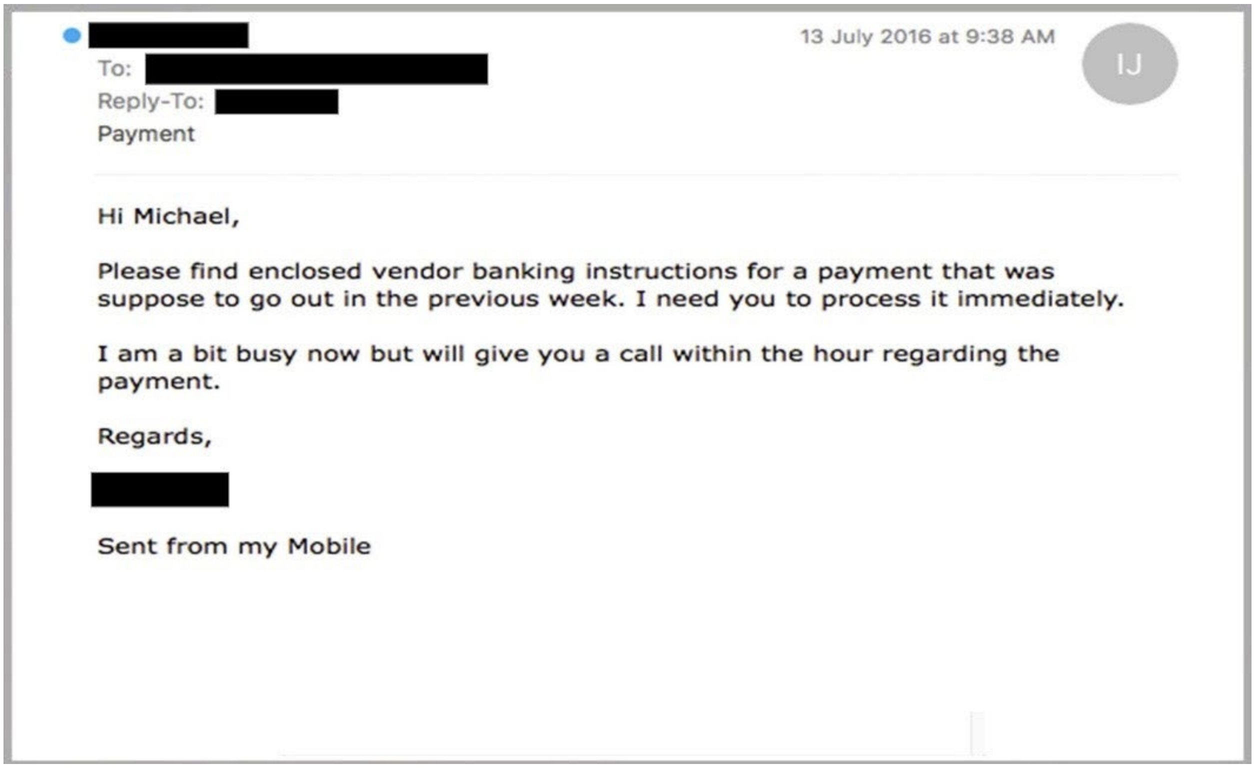
PayPal, Windows and Netflix all provide services that are regularly used, and any problems with those accounts could cause immediate inconveniences.

The business depends on you

The manufactured sense of urgency is equally effective in workplace scams.

Criminals know that an employee is likely to drop everything if their boss emails them with a vital request, especially when other senior colleagues are supposedly waiting on them.

A typical example looks like this:



[redacted]

To: [redacted]

Reply-To: [redacted]

Payment

13 July 2016 at 9:38 AM

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

Sent from my Mobile

Phishing scams like this are particularly dangerous because, even if the recipient did suspect foul play, they might be too afraid to confront their boss. This is tricky because after all, if they are wrong, they're essentially implying that there was something unprofessional about the boss's request.

But please remember it's better to be safe than sorry! Cyber-crime is real, and often very sophisticated and targeted towards businesses. We want to be sure you've got the tools to know what to look for and help keep you, your business and your team protected from this type of rapidly growing scam.

Source of training material: https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email

Password Security

The next topic we want to go over would be password control. Password security is something that we take very seriously and hackers out there that will not stop in order to hack someone's account. Here are some tips on how to create strong passwords, how to keep your passwords and accounts safe and how to help your team maintain safe and effective passwords, which in turn help protect your business.

How to create a strong password

Follow these tips to help yourself craft unique, complex passwords:

Do not use personal information.

1. Do not use your name or names of family members or pets in your passwords. Do not use numbers like your address, phone number, or birthdays, either. These can be publicly available, on forms you fill out or on social media profiles, and easily accessible to hackers.
2. Do not use real words
3. Password cracking tools are very effective at helping attackers guess your password. These programs can process every word in the dictionary, plus letter and number combinations, until a match is found. Steer clear of using real words from the dictionary or proper nouns or names.
4. Instead, use special characters. By combining uppercase and lowercase letters with numbers and special characters, such as “&” or “$,” you can increase the complexity of your password and help decrease the chances of someone potentially hacking into your account.

Create longer passwords

1. The longer the password, the harder it may be to crack. Try for a minimum of 10 characters.
2. Modify easy-to-remember phrases
3. One tip is to think of a passphrase, like a line from a song, and then use the first letter from each word, substituting numbers for some of the letters. For example: “100 Bottles of Beer on the Wall” could become “10oBb0tW”.
4. Do not write them down
5. Resist the temptation to hide passwords under your keyboard or to post them on your monitor. Stories about hackers getting passwords by rummaging through trash, also known as dumpster-diving, are absolutely real. And absolutely horrifying.
6. If you or someone on your team is going to be working in a remote, public area, make sure no one is watching or looking over your shoulder.

One way to store and remember passwords securely is to use a tool that keeps your list of usernames and passwords in encrypted form. Some of these tools, called password managers, will even help by automatically filling in the information for you on some websites. This comes in handy too, if you have shared platforms within your business.

Change passwords on a regular basis

1. Passwords for your online financial accounts should be changed every month or two. Computer login passwords should be changed at least once a quarter. Using the same password for longer periods could put your information at risk if a data breach occurs.
2. Use different passwords on different accounts
3. Do not use the same password on more than one account. If a hacker cracks it, then all of the information protected by that password on other accounts could also be compromised. Use a password generator, like Norton Identity Safe, to help create unique and strong passwords.
4. Do not type passwords on devices or networks you do not control

Never enter your password on another person's computer. It could be stored without your knowledge.
When using your devices on public Wi-Fi, you should avoid visiting websites that require you to log in to your account, such as online banking or shopping. When you're on an unsecured public network, your unencrypted data could be intercepted by a nearby hacker. To protect yourself from these threats, you should always use a virtual private network (VPN), like Norton Secure VPN, when on a public Wi-Fi connection.

How to maintain a secure account

Two-factor authentication, or 2FA, is a method of verifying your identity that adds a second layer of security to your account password. Types of two-factor authentication can include any of the following:

1. Something you know: a PIN number, password, or pattern
2. Something you have: an ATM or credit card, mobile phone, or security token
3. Something you are: a biometric form of authentication, such as your fingerprint, your voice, or your face

How to use a password manager and ease the mind of your clients

Password managers are services that auto-generate and store strong passwords on your behalf. This is ideal for sharing passwords with others in your business setting. These passwords are kept in an encrypted, centralized location, which you can access with a master password. (Don't lose that one!) Many services are free to use and come with optional features such as syncing new passwords across multiple devices and auditing your password behavior to ensure you are not using the same one in too many locations.

Platform Suggestions

Some great ones to use for your clients are:
1. Lastpass
2.Dashlane
3.1password
4. Roboform
5. Stickypassword
6. Nordpass

The best thing about using a password manager is that you do not have to provide anyone with a physical password. You can simply state share with another party (employee or team member, client, etc) and then that one password is encrypted and sent into their password manager (they do have to be on the same platform for this to work). This is a safe, free and easy to use solution to password management. In the event of an employee or client departure, you would simply unshare that, and they would no longer have access to it. Safe, quick and easy.