As of late, we have been seeing much more "spam", phishing emails, malware and other security risks.  The purpose of this document is to go over some of the examples that can pop into your inbox and the ways you can protect not only yourself but your clients too.

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.

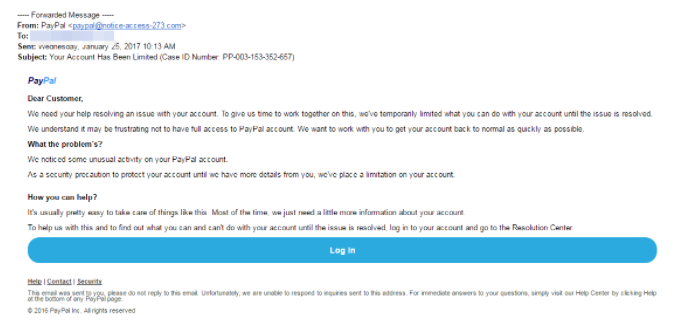
Here are some things to look for when receiving an email from someone new:

***1. The message is sent from a public email domain.***

 Examples of this are:

* No legitimate organization will send emails from an address that ends ‘@[gmail.com](http://gmail.com/)’.
* Not even Google.
* Most organizations, except some small operations, will have their own email domain and company accounts. For example, legitimate emails from Google will read ‘@[google.com](http://google.com/)’.
* If the domain name (the bit after the @ symbol) matches the apparent sender of the email, the message is probably 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**



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](mailto:paypal@notice-access-273.com)’.

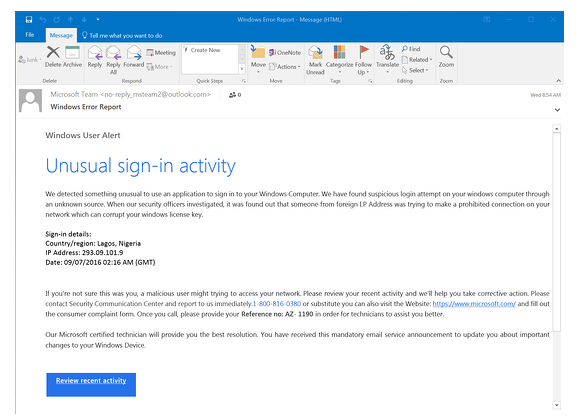
***2. The domain name is misspelled***

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.

***3. 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 only the most gullible 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**



It’s therefore the recipient’s responsibility to look at the context of the error and determine whether it’s a clue to something more sinister. You can do this by asking:

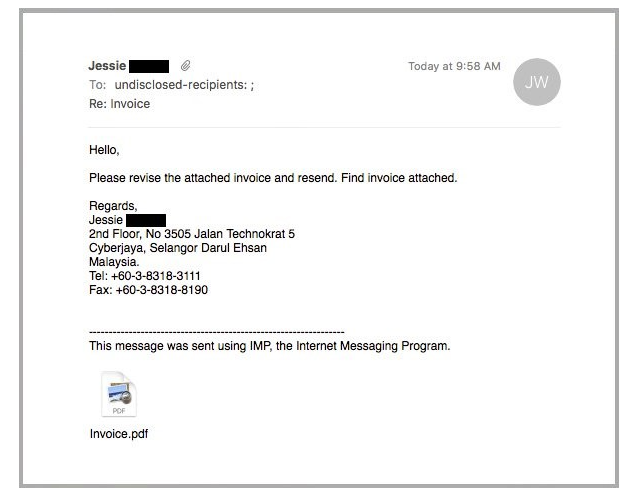
* Is it a common sign of a typo (like hitting an adjacent key)?
* Is it a mistake a native speaker shouldn’t make (grammatical incoherence, words used in the wrong context)?
* Is this email a template, which should have been crafted and copy-edited?
* Is it consistent with previous messages I’ve received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

***4. It includes suspicious attachments or links***

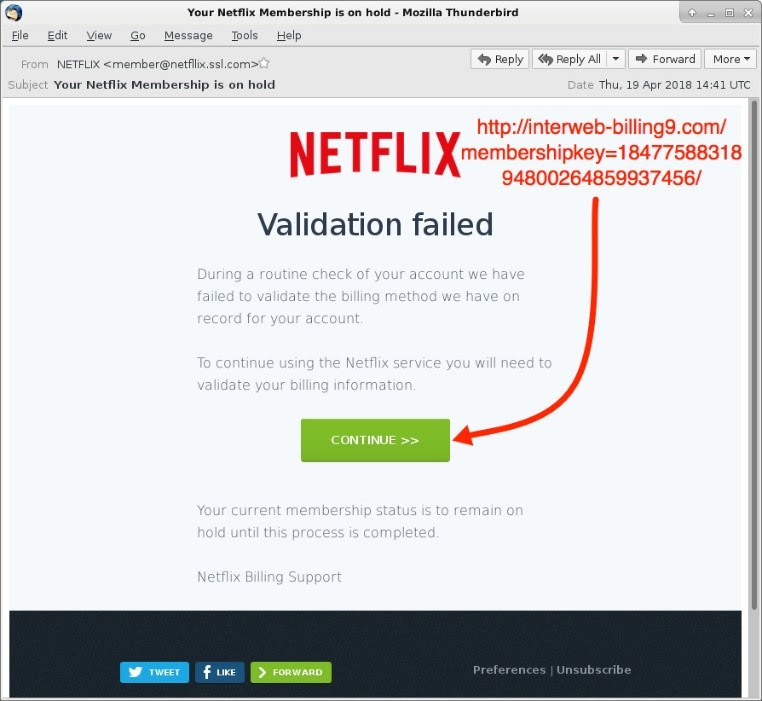
Phishing emails can come in many different forms including social media posts and text messages. But no matter how phishing emails are delivered, they all contain a payload. This will either be an infected attachment that you’re asked to download or a link to a bogus website.  
  
The purpose of these payloads is to capture sensitive information, such as 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:



It doesn’t matter whether the recipient expects to receive an invoice from this person or not, because in most cases they won’t be sure what the message pertains to until they open the attachment.  
  
When they open the attachment, they’ll see that the invoice isn’t intended for them, but it will be too late. The document unleashes malware on the victim’s computer, which could perform any number of nefarious activities.

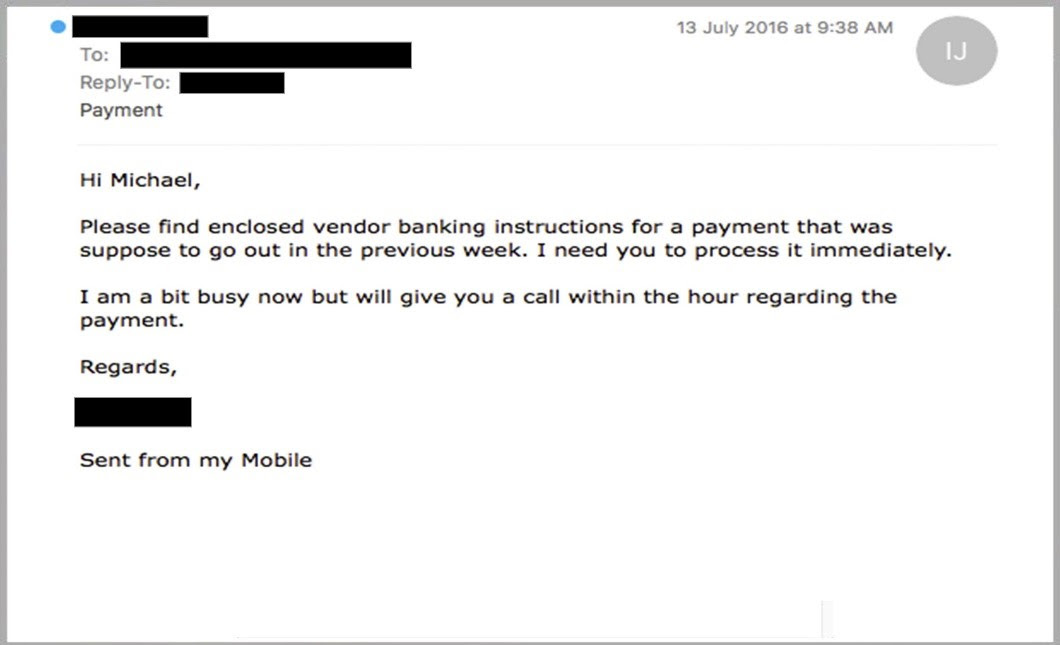
***Suspicious links***  
  
You can spot a suspicious link if the destination address doesn’t match the context of the rest of the email.  
  
For example, if you receive an email from Netflix, you would expect the link to direct you towards an address that begins ‘[netflix.com](http://netflix.com/)’.  
  
Unfortunately, many legitimate and scam emails hide the destination address in a button, so it’s not immediately apparent where the link goes to.



***5. The message creates a sense of urgency***  
  
Scammers know that most of us procrastinate. We receive an email giving us important news, and we decide we’ll deal with it later.  
  
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 we’re likely to drop everything if our boss emails us with a vital request, especially when other senior colleagues are supposedly waiting on us.  
  
A typical example looks like this:



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

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 work with a client who is nervous about sharing passwords with their VA.

***How to create a strong password***  
  
Follow these tips to help yourself craft unique, complex passwords.

1. Do not use personal information
2. 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.
3. Do not use real words
4. 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.
5. 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.
6. When you type your password in a public setting, 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.  
  
***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. Don’t 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. 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.

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 your clients do not have to provide you with the physical passwords. They can simply state share with you and then that one password is encrypted and sent into your password manager (they do have to be on the same platform for this to work). This works with a lot of our clients as it's safe, free and easy to use. If the client steps away from VA USA, they can simply unshare that password and you would no longer have access to this. This is something that we often bring up on client calls as some are not aware of it