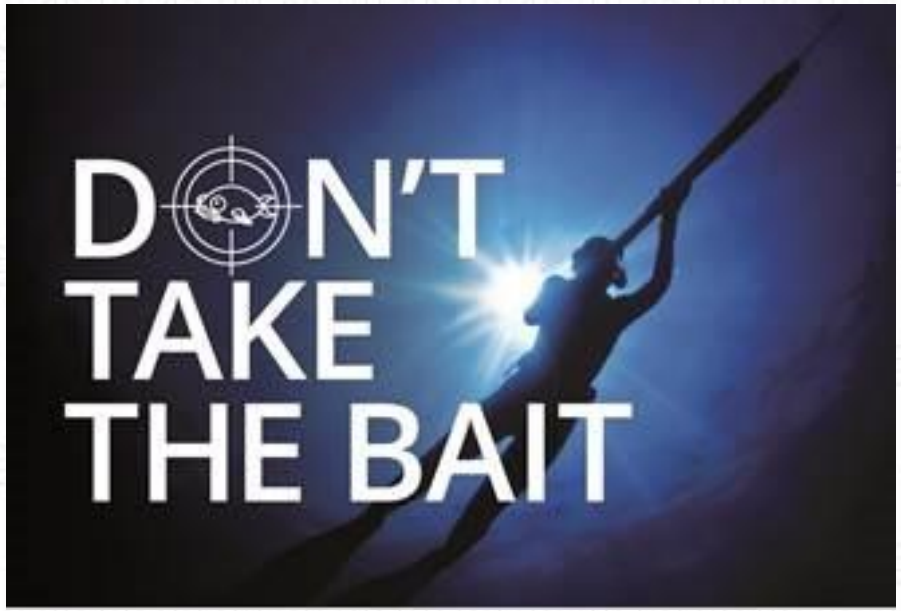
TBK BANK

INFORMATION SECURITY AWARENESS
PHISHING

PHISHING

- Phishing is when a scammer uses fraudulent emails, texts, or copycat websites to get you to disclose valuable personal information – such as account numbers, Social Security numbers, or your usernames and passwords.
- Phishing is akin to fishing in a lake, but instead of trying to capture fish, phishers attempt to capture your personal and login information.
- Phishing is the #1 cause of data breaches.



WHOSE PHISHING?

- Cybercriminals
- Hacktivists
- Military and State Sponsored Hackers



PRIVACY AND FINANCIAL LOSS

Personal Identifiable Information

- Social Security Numbers
- Drivers' License Numbers
- Addresses
- Birth Dates
- Health Records
- Account Numbers

Impact

- Criminals can apply for loans or credit cards on your behalf
- Intercept your tax returns and receive government benefits
- Use your health benefits to purchase medication or receive service
- File fraudulent insurance claims
- Empty your bank account

EXTORTION

- Denial of Service Attack
  - Attack used to disrupt services to prevent legitimate access
- Ransomware
  - Attack in which malware encrypts the victims data preventing access. The perpetrator then offers up the decryption key in exchange for money.
- Pay or Not to Pay?
  - Will you actually receive the key if you pay?

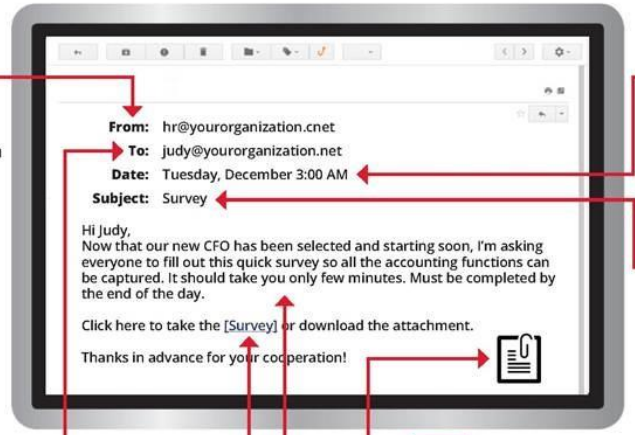


SOCIAL ENGINEERING RED FLAGS

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**.

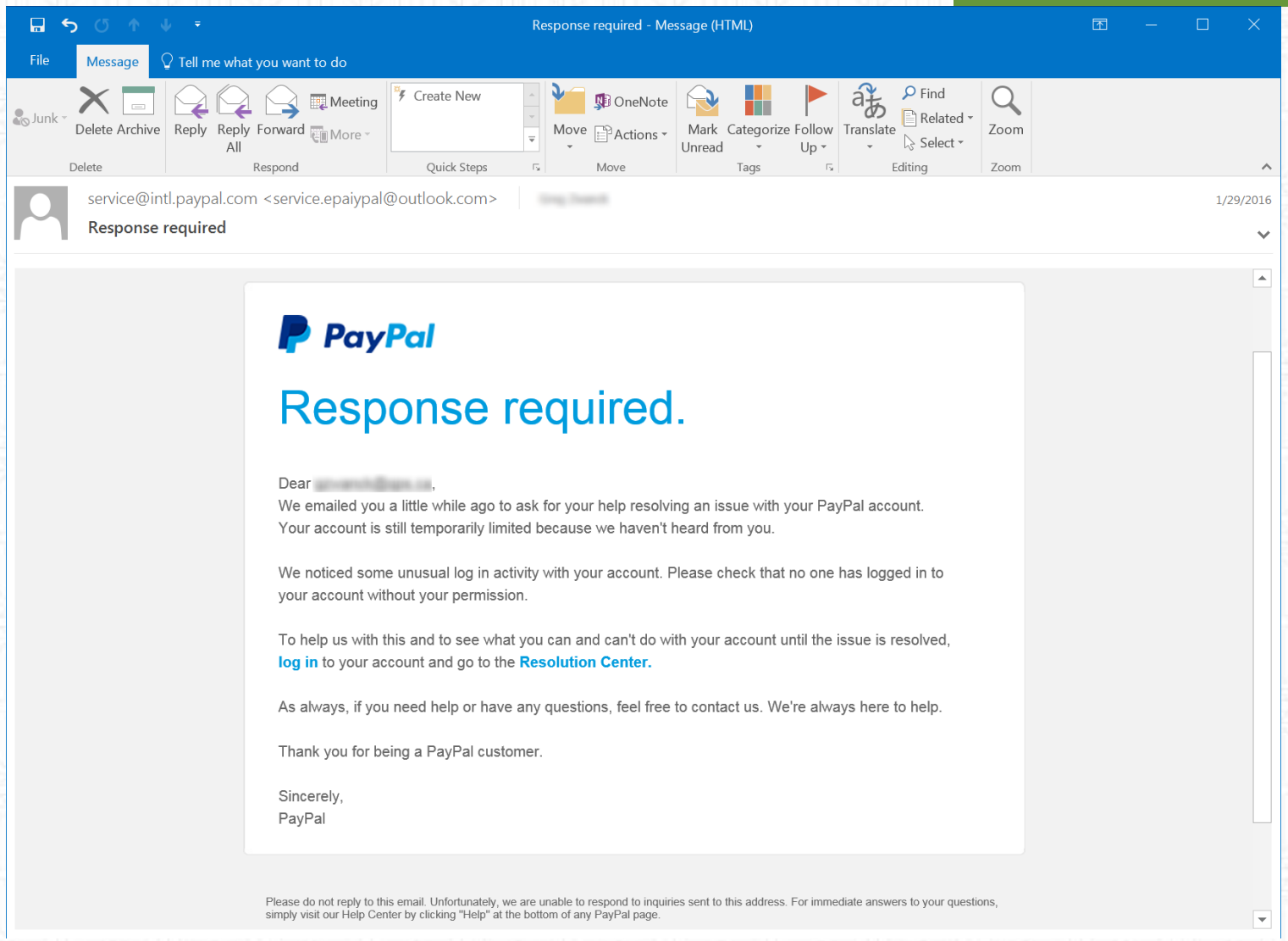
HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known website. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

CONTENT

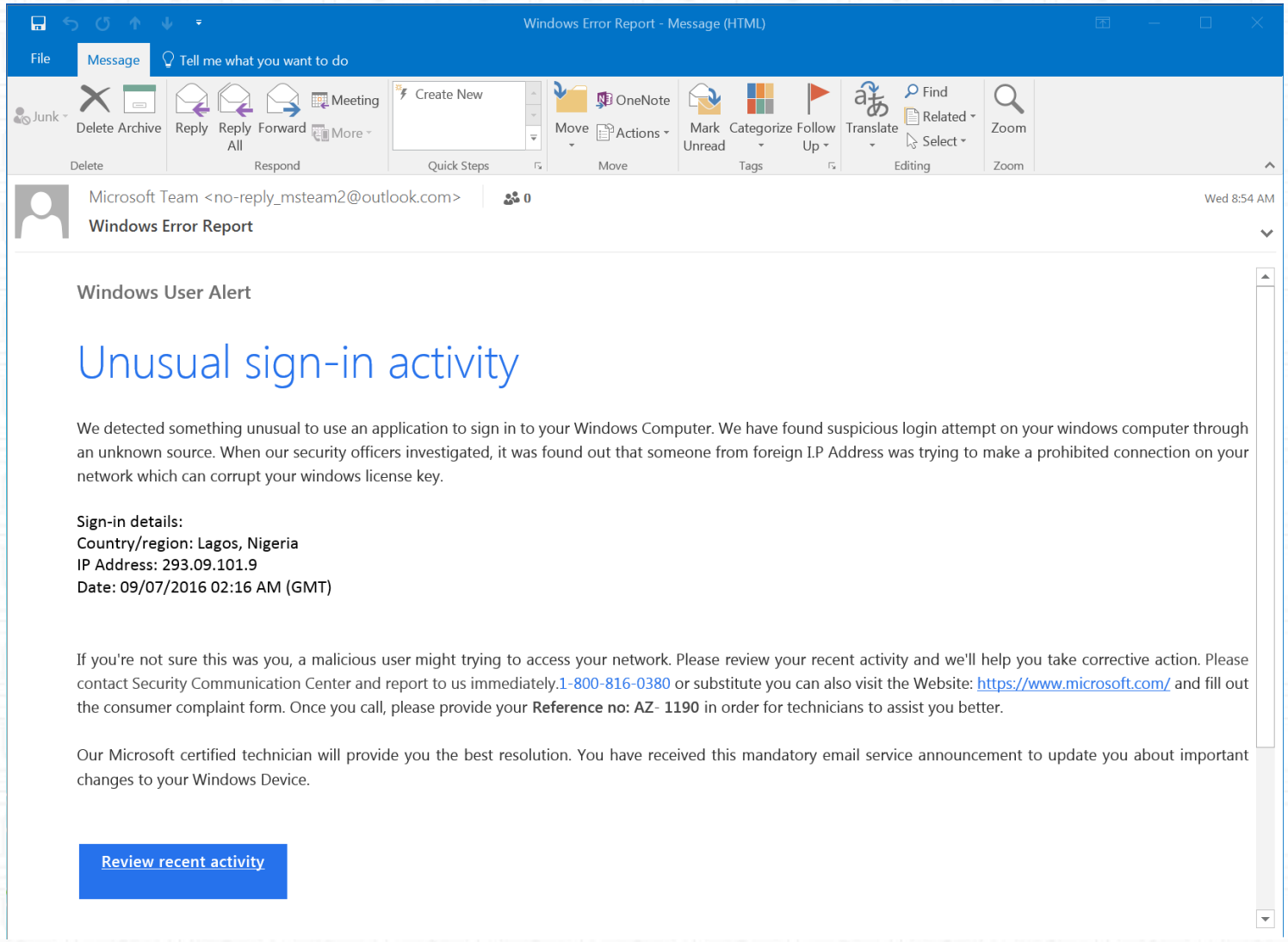
- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

PHISHING EXAMPLES



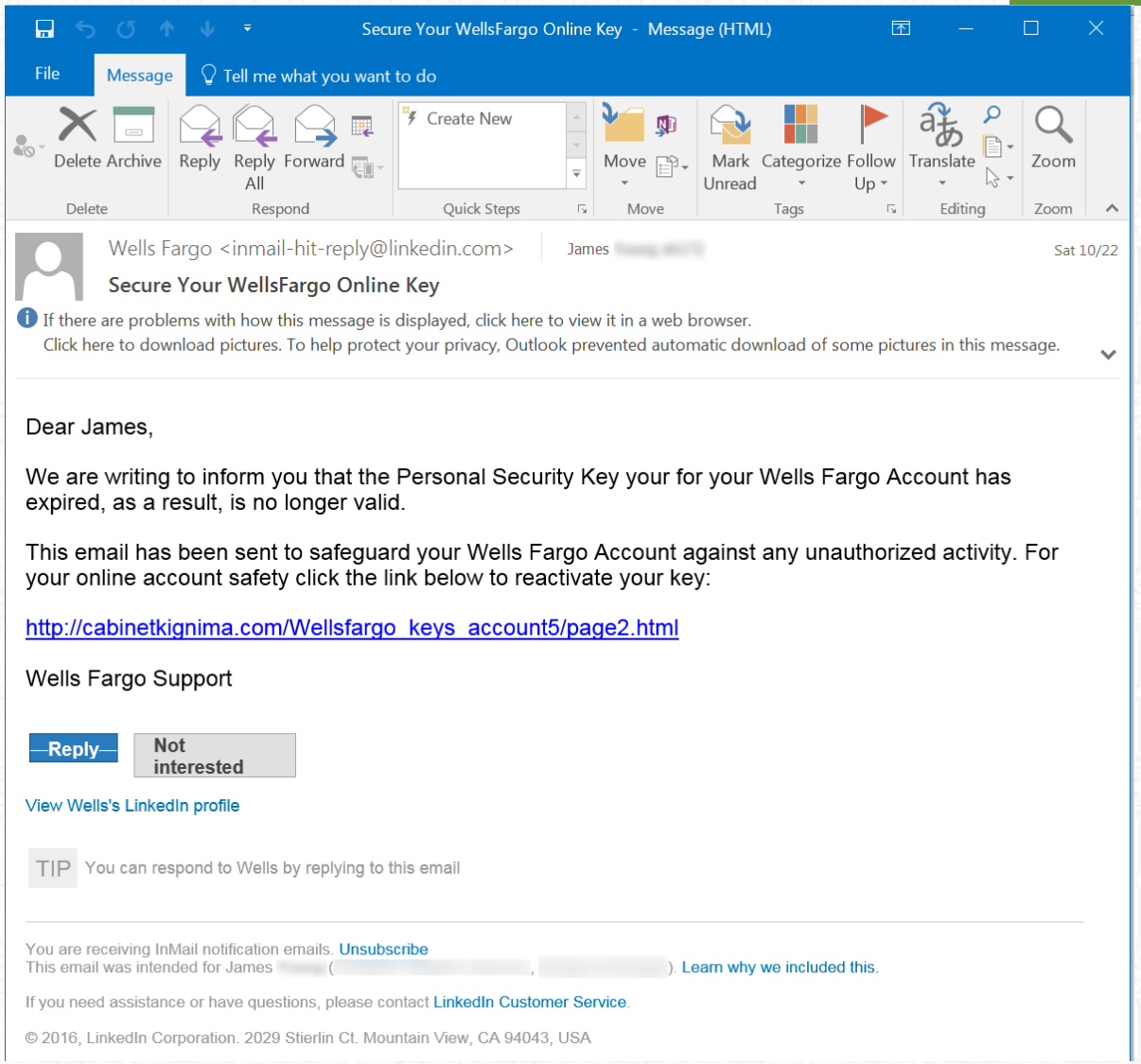
- service.epairypal@outlook.com is not a legitimate email address for PayPal support.
- Links in the email don't point to PayPal if you hover your mouse over them.
- If you are concerned with there actually being a issue with your account, the best thing to do in this scenario is to go directly to paypal.com and sign in, don't follow the links.

PHISHING EXAMPLES



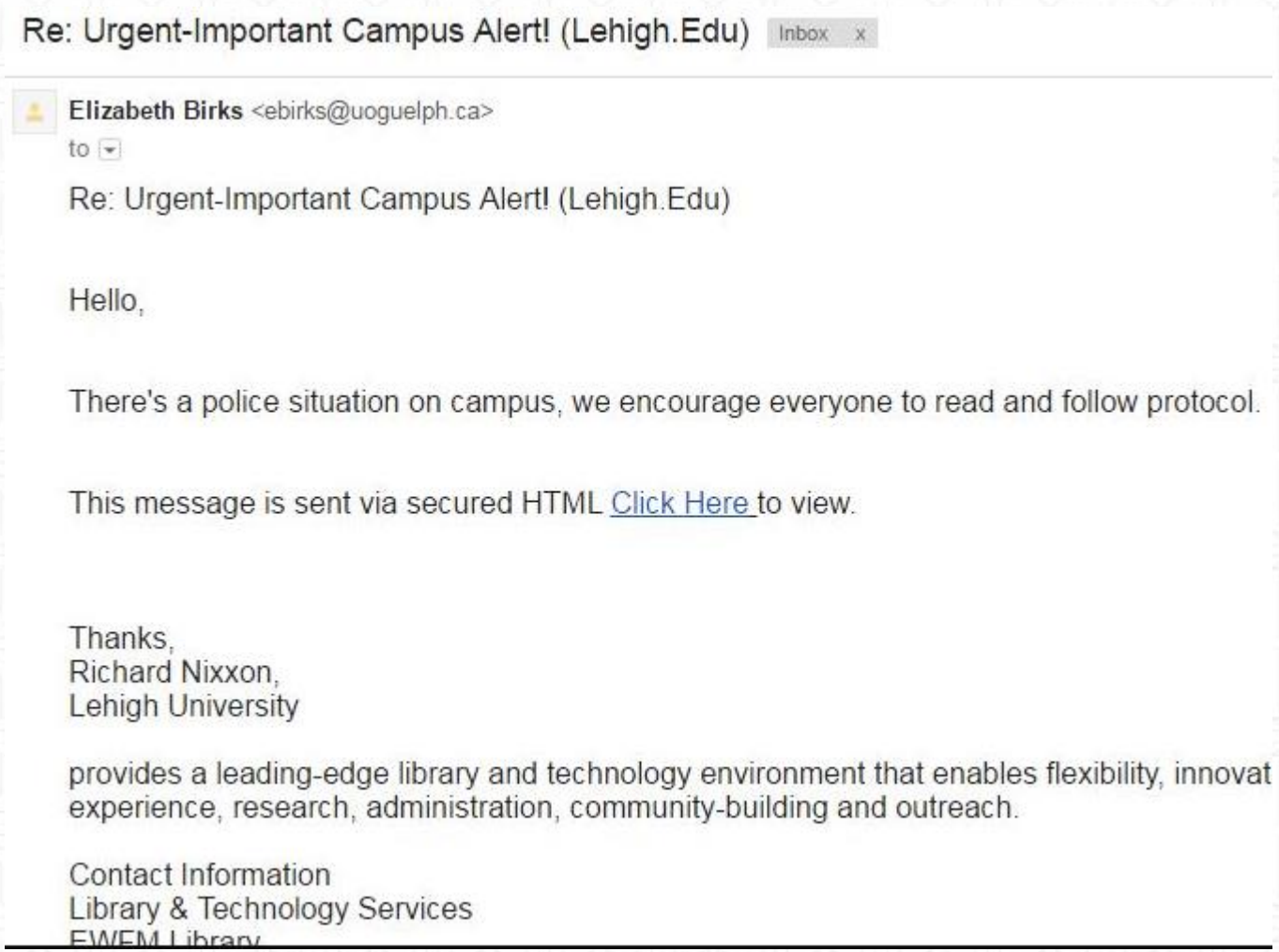
- No-reply_msteam2@outlook.com is not a legitimate Microsoft Support email address.
- The grammar in the email is off
- Hovering over the links shows that they go to non Microsoft websites

PHISHING EXAMPLES



- Inmail-hit-reply@linkedin.com is not a valid Wells Fargo email address.
- The included link is going to an unusual location. It takes you to “Cabinetkignima.com” not Wells Fargo.

PHISHING EXAMPLES



Re: Urgent-Important Campus Alert! (Lehigh.Edu) Inbox x

Elizabeth Birks <ebirks@uoguelph.ca>
to

Re: Urgent-Important Campus Alert! (Lehigh.Edu)

Hello,

There's a police situation on campus, we encourage everyone to read and follow protocol.

This message is sent via secured HTML Click Here to view.

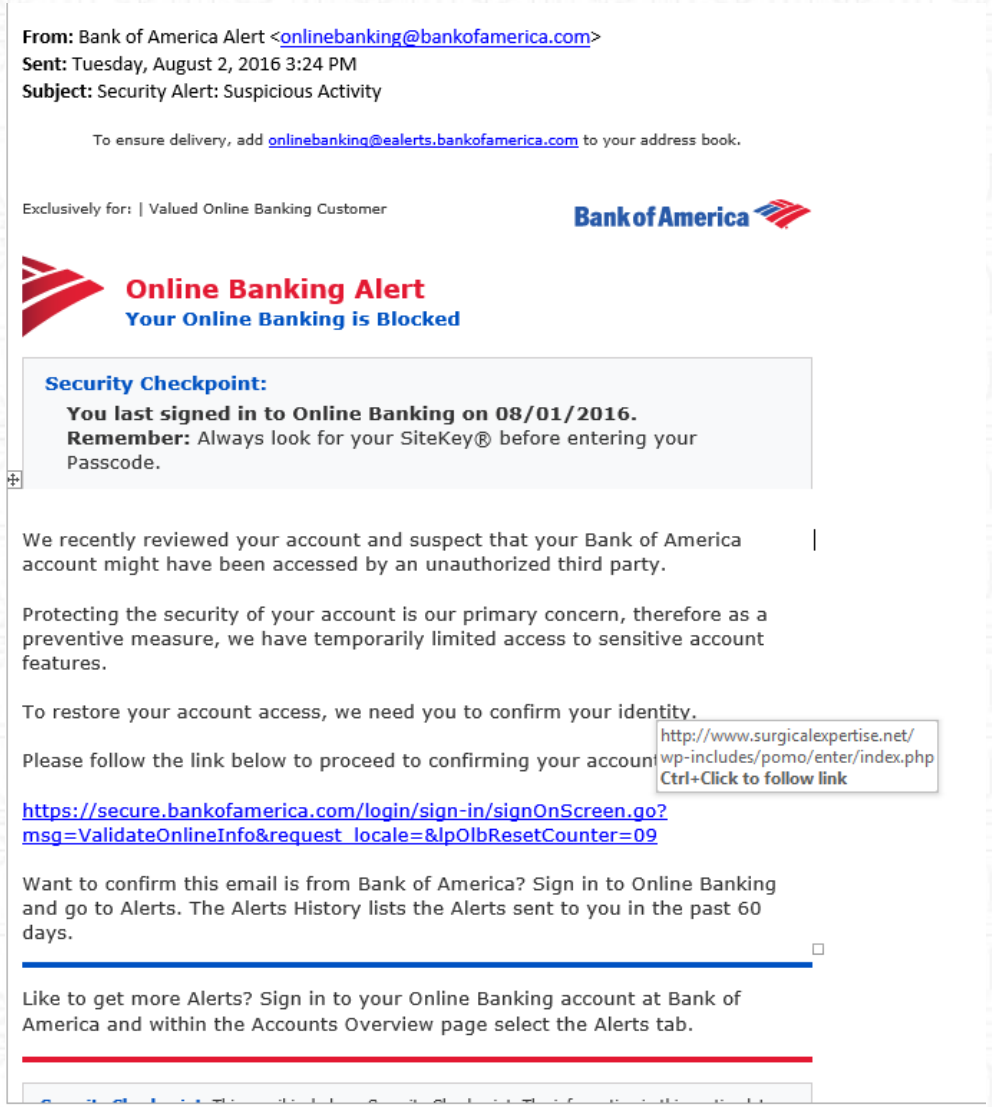
Thanks,
Richard Nixxon,
Lehigh University

provides a leading-edge library and technology environment that enables flexibility, innovat
experience, research, administration, community-building and outreach.

Contact Information
Library & Technology Services
EWEM Library

- This phishing email implores a sense of urgency to try and distract you from analyzing the email.
- Always stop and take a moment to critically think before clicking. Does the address look safe if you hover your mouse over the link? Should you be receiving this type of email or is it relevant to you? When in doubt, ask!

PHISHING EXAMPLES



From: Bank of America Alert <onlinebanking@bankofamerica.com>
Sent: Tuesday, August 2, 2016 3:24 PM
Subject: Security Alert: Suspicious Activity

To ensure delivery, add onlinebanking@ealerts.bankofamerica.com to your address book.

Exclusively for: | Valued Online Banking Customer

Bank of America

Online Banking Alert
Your Online Banking is Blocked

Security Checkpoint:
You last signed in to Online Banking on 08/01/2016.
Remember: Always look for your SiteKey® before entering your Passcode.

We recently reviewed your account and suspect that your Bank of America account might have been accessed by an unauthorized third party.

Protecting the security of your account is our primary concern, therefore as a preventive measure, we have temporarily limited access to sensitive account features.

To restore your account access, we need you to confirm your identity.

Please follow the link below to proceed to confirming your accoun

http://www.surgicalexpertise.net/wp-includes/pomo/enter/index.php
Ctrl+Click to follow link

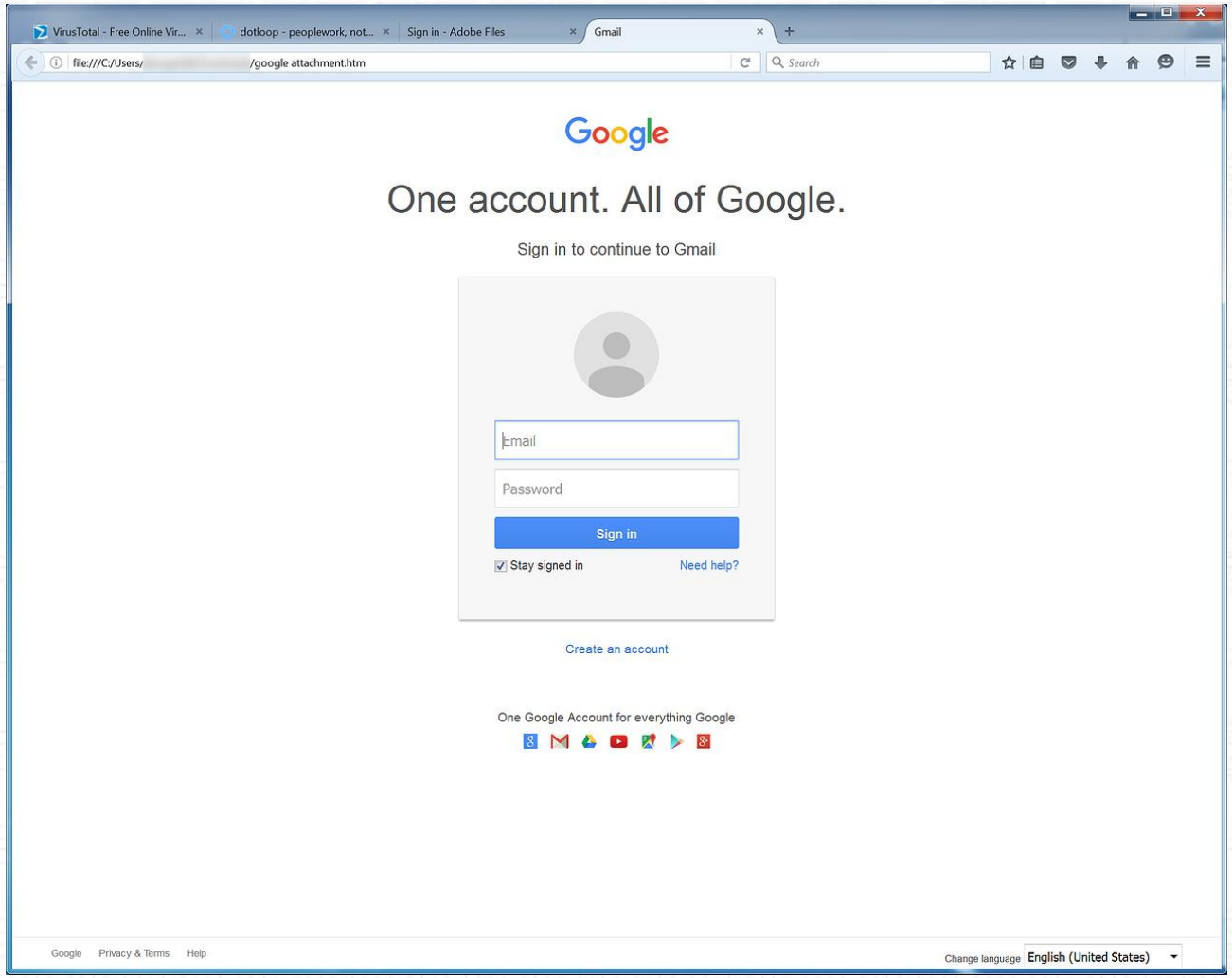
https://secure.bankofamerica.com/login/sign-in/signOnScreen.go?msg=ValidateOnlineInfo&request_locale=&IpOlbResetCounter=09

Want to confirm this email is from Bank of America? Sign in to Online Banking and go to Alerts. The Alerts History lists the Alerts sent to you in the past 60 days.

Like to get more Alerts? Sign in to your Online Banking account at Bank of America and within the Accounts Overview page select the Alerts tab.

This is a sneaky one, the email address was spoofed to make it appear to be coming from a legitimate address. Most of the hyperlinks also go to Bank of America. The only suspicious item is the link that says it's going to secure.bankofamerica.com. By hovering the mouse over that link, we can see that it's actually going to www.surgicalexpertise.net. There's no way that's legitimate.

HTML ATTACHMENTS

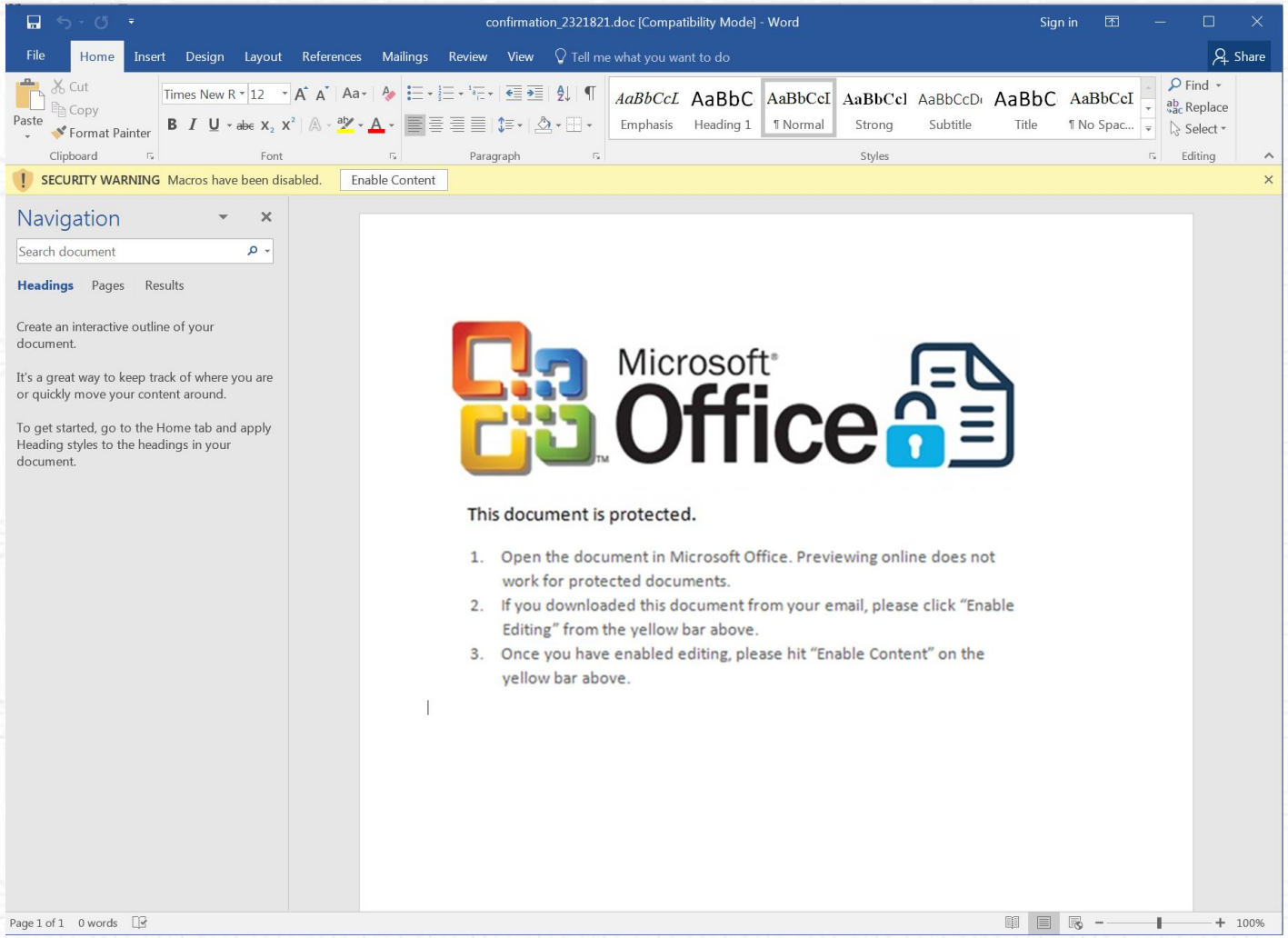


Sometimes people will attach HTML files to an email. This can be a completely self contained webpage that will open with your web browser.

In this example, we've got a page that looks exactly like the sign-in screen for a google account. If someone makes the mistake of putting in their credentials on this page and tries to sign in, their credentials will be sent to the attacker instead. Afterwards they may even re-direct you to the actual google login page to make it seem like nothing malicious happened on your end.

Before signing into anything online, verify the url is what it should be.

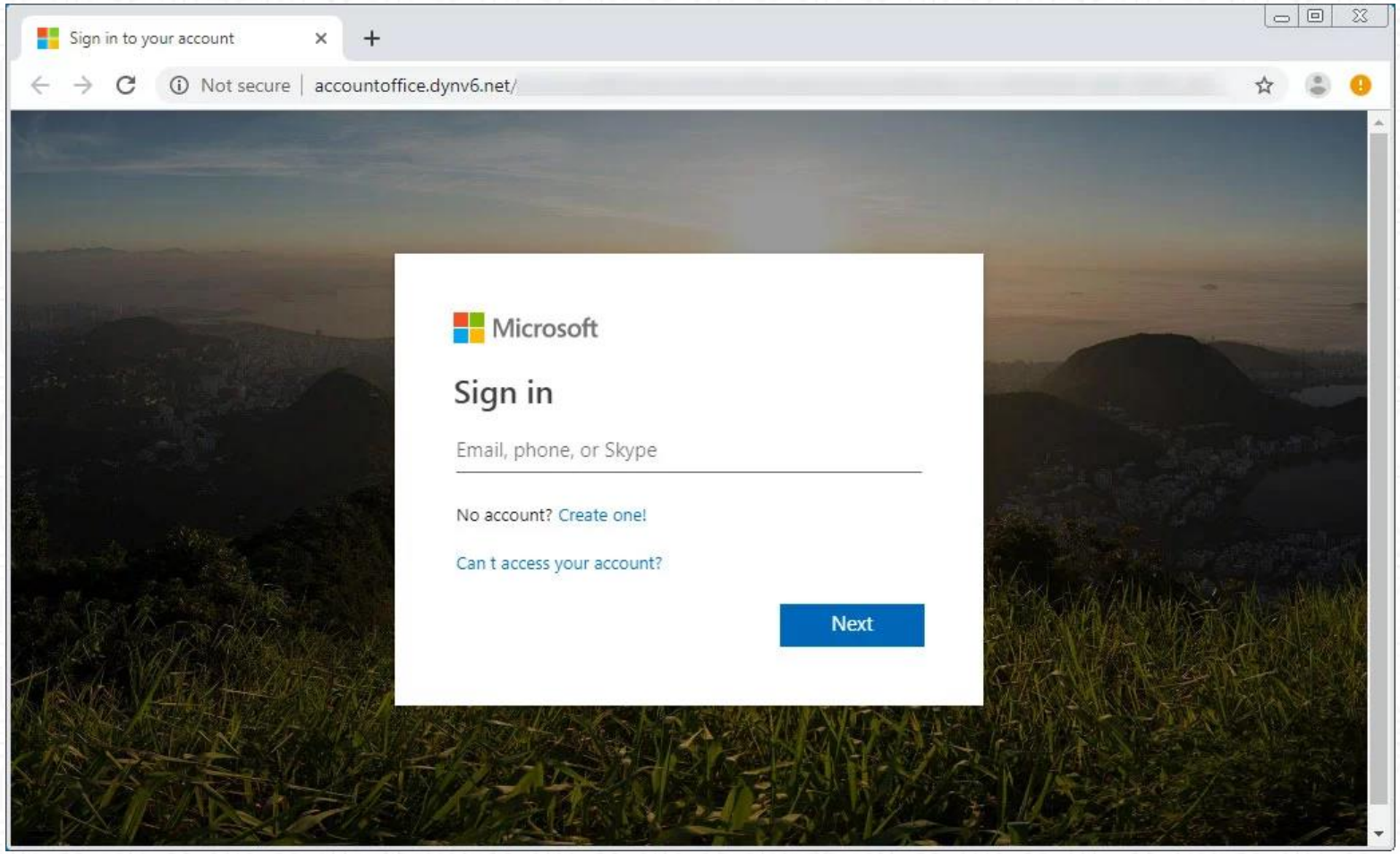
ATTACHMENTS WITH MACROS



Attachments with Macros can be particularly dangerous. A macro will allow a script or series of commands to run automatically. While this can be useful for doing repetitive tasks in Microsoft documents, it's also useful for malicious actors.

If you enable the macro, that can execute the malware, download additional files onto the computer, or even gather information.

SPOOFED WEBSITES



- It's trivial for a threat actor to create a fake website. Oftentimes they will borrow elements from the site they are spoofing to make it look exactly the same. In this example we know this is a fake website because of the url. accountoffice.dynv6.net isn't affiliated with Microsoft.
- How would you know that? Sometimes you won't. The best way to avoid falling for sites like these is to not follow links in emails, texts, or social media posts, but instead go directly to the source. Type in Microsoft.com in your web browser then click "Sign in"

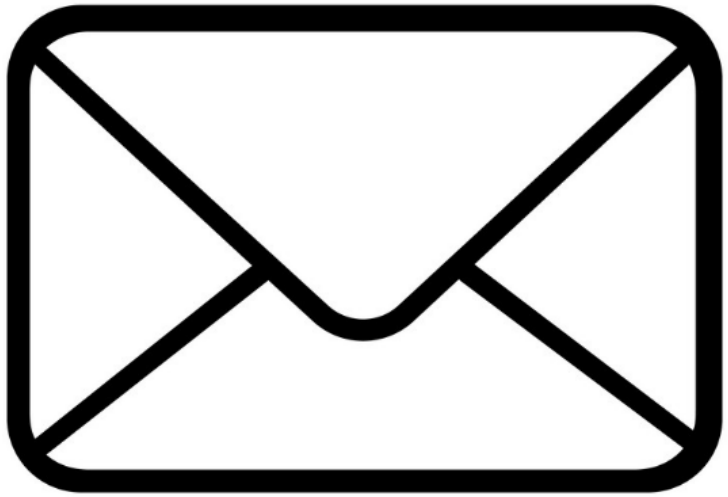
STAYING SAFE BEYOND PHISHING

- Looking out for Phishing emails is only one of many precautions that you can take to keep information secure. Remember these practices can also be applied outside of work. Your personal information at home can be just as important.



SENDING EMAILS SECURELY

- Check that you're sending to the correct email address. Outlook's auto-complete function could have filled in the wrong address.
- Check for information in the email that you don't actually want to send. Maybe you accidentally copied something that wasn't intended.
- Check if there is confidential information that shouldn't be leaving the corporate network at all.
- Is there private information in the email that should be encrypted? If so use Zix or Egnyte if you're at work. TED has instructions on this.



BEWARE OF MALWARE

- Cyber criminals install malware on your computers or devices to gain control over them. Once installed, malware can enable criminals to spy on your online activities, steal your passwords or files, take control of your files, or use your system to attack others. Malware can infect any device, from computers (Mac included) and smartphones to DVRs and security cameras.
- Be careful of what you install on your electronic systems
- Keep those systems up to date
- Install antivirus and keep it updated
- Be careful when following links!



SECURE YOUR MOBILE DEVICES

- Enable automatic updating on the device so they are always running the latest version of the operating system and applications.
- Enable automatic locking of the screen with a password, PIN, or fingerprint. That way no one can easily access your device if it's lost or stolen.
- Enable or install software to remotely track your mobile device. This can help you find a lost phone, or in the event of theft, allow you to remotely wipe the device.



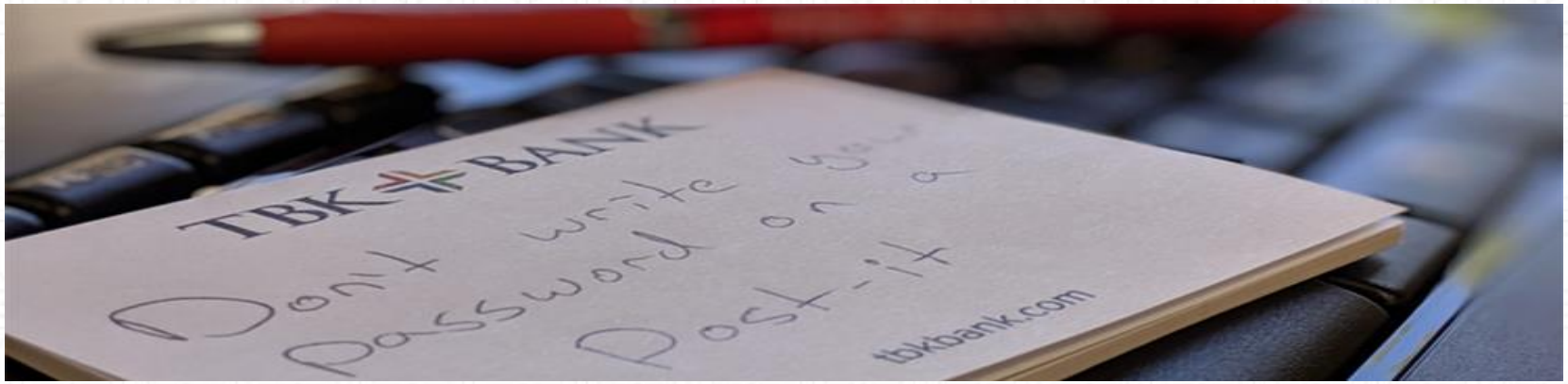
SECURE YOUR MOBILE DEVICES CONTINUED

- Only install applications from trusted sources and don't "root" or "jailbreak" your phone. Bad apps can still appear in the official marketplaces, be wary of brand new applications with few reviews from an unknown developer. When you find yourself not using the app anymore, uninstall it. This will free up space and remove a potential vulnerability.
- Turn on automatic backups. Most providers offer a free storage tier, take advantage of it! If you replace your phone, this helps make the transition much easier.
- Be careful with links in text messages and emails. Just because you're on a phone doesn't mean you can't become compromised by a malicious link.



PASSWORDS

- When creating a password, consider using a Passphrase. A Passphrase is much easier to memorize and if sufficiently long, makes it significantly harder to brute force. The key is to use a phrase that would not appear in any normal conversation. Then throw in a number or symbol to meet password complexity requirements.
  - SaxaphoneHappyPickleStew2#
- If you aren't using a passphrase, avoid using common words that would be found in a dictionary (any language) and using personal information. Things like important dates or pet names are very easy to discover on social media.
- Never use a password more than once. If a password becomes compromised due to a data breach or other means, attackers will try those credentials on other web services to see if you are using the same password. If you are, that service becomes compromised as well.
- Enable MFA (Multi Factor Authentication) wherever available.
- Change your passwords often, especially if you suspect it's been compromised.
- Don't share your passwords, ever! Even with IT!

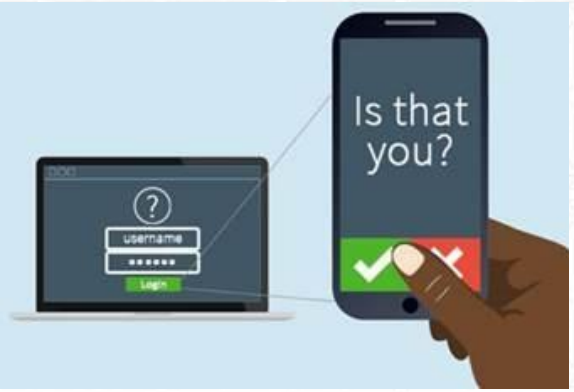


MULTI FACTOR AUTHENTICATION (MFA)

Login credentials can generally be grouped into 3 different types of categories:

Something you know	Something you have	Something you are
• Password • Passphrase • Pin number	• Security Token • MFA App on Phone • Text Confirmation	• Fingerprint reader • Facial recognition • Palm Scanner

- Multi-factor authentication or MFA, is a security procedure that requires two or more independent credentials from these categories. Using a Pin number and a Password doesn't count, they have to be from separate categories.
- If your password becomes compromised due to a data breach or by other means, someone with that password still can't sign in unless they have the other MFA credentials.



- Some forms of authentication are stronger than others (SMS texts have many insecurities), but always keep in mind nothing is 100% secure.
- That being said, you should still enable MFA wherever possible. The more layers in place, the more difficult it is for someone to gain unauthorized access.

DATA BREACHES

What is a Data Breach?

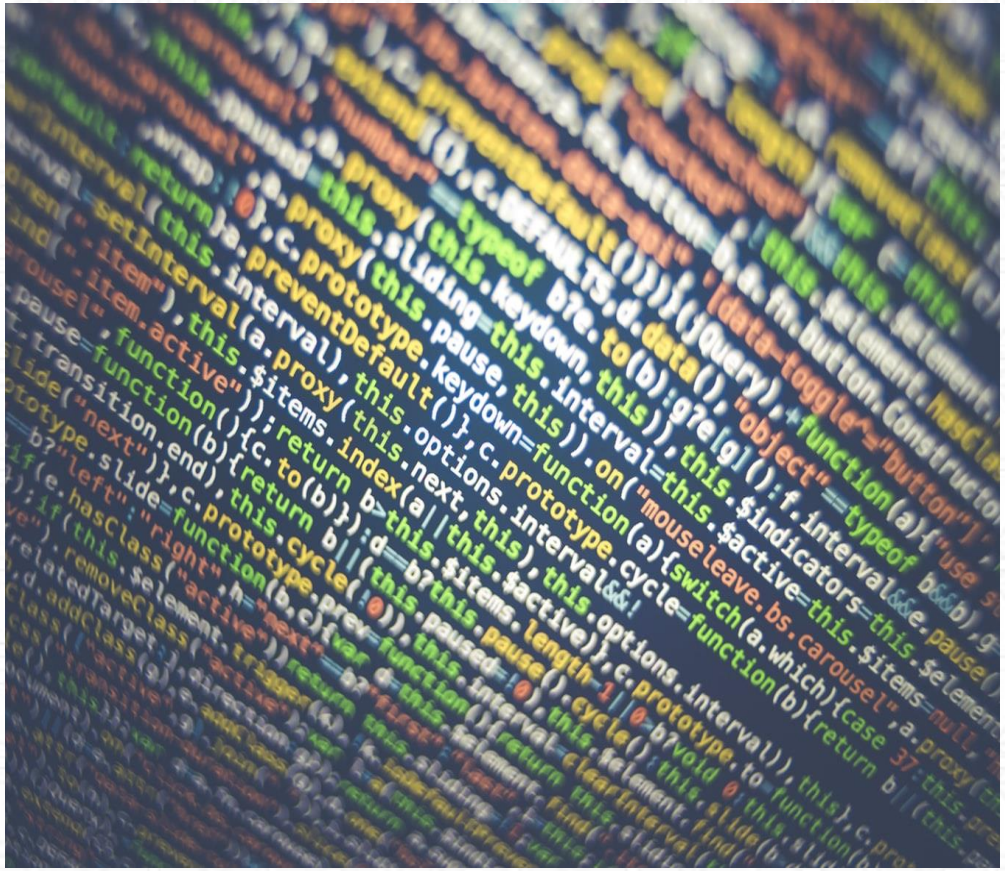
- A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. When we hear about Data Breaches in the news, they generally are related to user login information. How can you keep up and find out if you're the victim of a massive data breach?
- Here are two projects that can help you tell:
  https://haveibeenpwned.com/
  https://breachalarm.com/
- After you input the email you are concerned about, the site will check if that email is found in one of the analyzed data breaches. Never input your password into a tool that checks for leaked passwords.



DATA BREACHES CONTINUED

What should you do if you are the victim of a Data Breach?

- If your primary email account credentials are compromised, start with that account first. Change your password as soon as possible to something unique and take this opportunity to activate two-factor authentication (where available) if you haven't yet. Then move on to any other potentially compromised accounts.
- If you use the compromised password anywhere else (hopefully you're not) then you must change it everywhere else you use it. The first thing someone with your password will do is attempt to login with the same credentials on other sites and services to compromise as many accounts as possible.
- This is why having a different password for every login is so important. If your credentials become compromised, you'll only have to worry about the one account being affected.



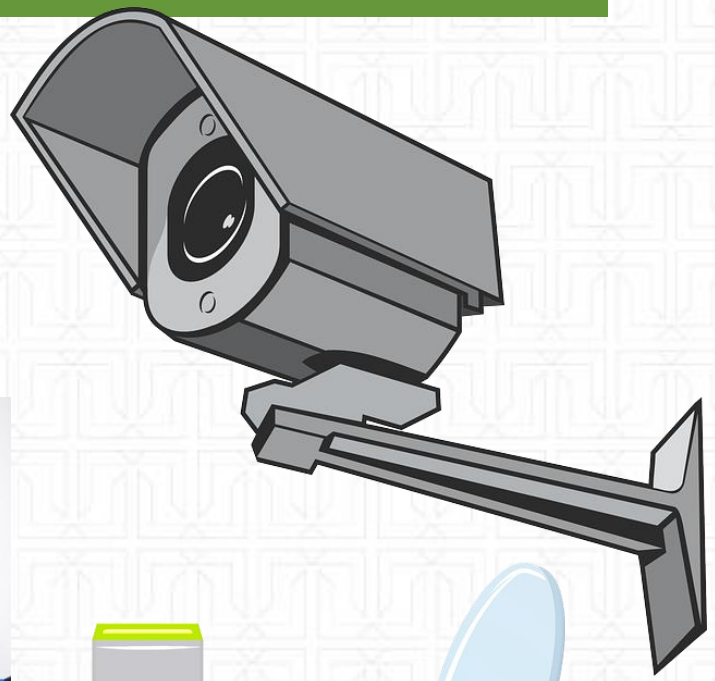
PUBLIC WIFI

- A public Wi-Fi network is inherently less secure than your personal private one, because you don't know who set it up, or who else is connecting to it.
- Stick to websites that have https in the URL, if a website is only http, it’s trivial for someone on the same network to capture the data that travels between you and the server your connecting to.
- Disable network sharing on public networks
- Use a VPN if you have access to one, or connect to cellular with your phone if you must do something securely, like signing into your bank account. Beware of data usage if you don’t have an unlimited data plan.



INTERNET OF THINGS (IOT)

- Many things besides computers and phones connect to the internet.
  - Security Systems
  - Cameras
  - Air-conditioning controllers
  - Refrigerators
  - Internet Routers







- Staying Secure
  - Change default usernames and passwords
  - Keep the devices up to date
  - Verify settings and permissions
  - Watch out for off-brand or knock-off items

SUMMARY

- Cybersecurity starts with you
  - Protect PII
  - Be wary of every email that comes in
  - Scrutinize all fields in an email
  - Be very careful with links and attachments
  - Report phishing emails to the helpdesk or information security
  - Encrypt sensitive emails
  - Be careful what applications you install
  - Keep your systems up-to-date. Computers, phones, cameras, toilets, etc…
  - Have different passwords and change them regularly
  - Enable MFA
  - Don’t trust Public WiFi
  - Change the default username and passwords on your devices