



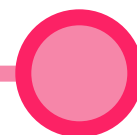
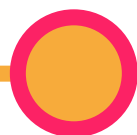
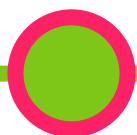
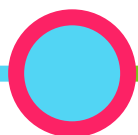
Bridging Digital Gaps

Presented By: RIWC

Series Progress



Learning About
Online Scams



Taking a look at the
different types of fraud
and scams on the
internet

Today's Agenda

1. Learning about different online scams

2. Learning how to identify scams

3. Learning about current preventions

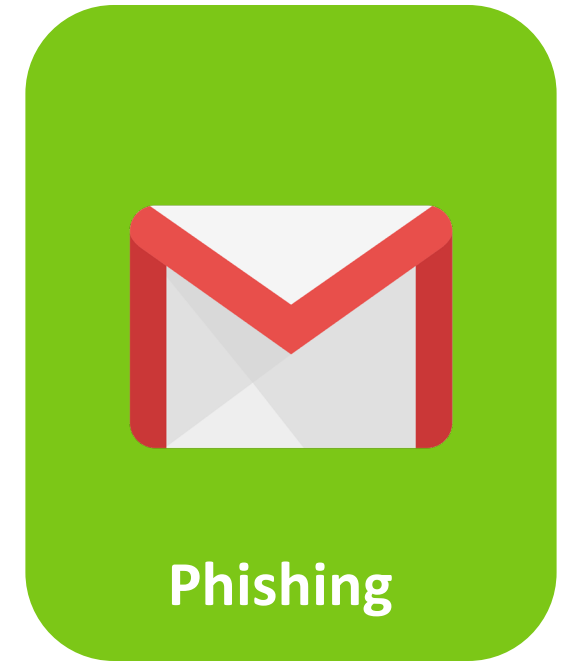
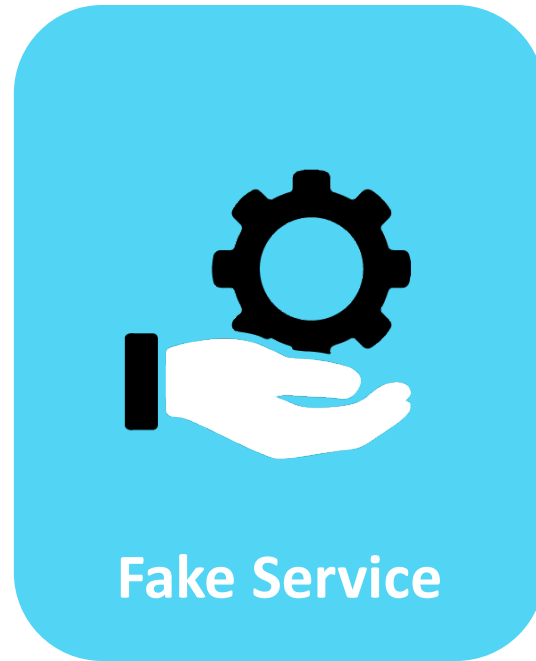
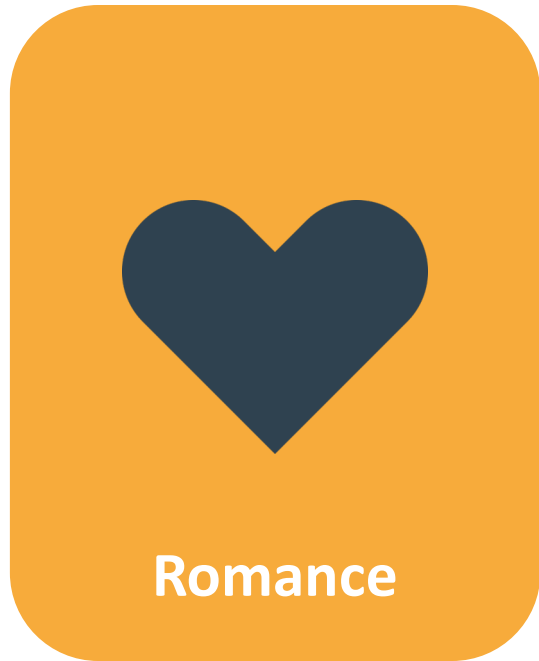


Land Acknowledgement

We acknowledge that we are on the traditional territory of many nations including the Mississaugas of the Credit, the Anishinaabeg, the Chippewa, the Haudenosaunee and the Wendat peoples and is now home to many diverse First Nations, Inuit and Métis peoples. We also acknowledge that Toronto is covered by Treaty 13 signed with the Mississaugas of the Credit, and the Williams Treaties signed with multiple Mississaugas and Chippewa bands. This land is also governed by the dish with one spoon wampum belt convenient: an agreement between allied First Nations to peaceable share and care for the land around the Great Lakes.

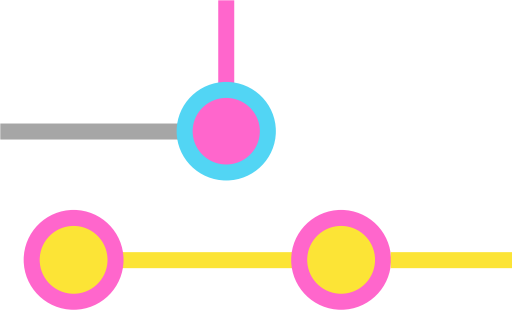
The City of Toronto has been acknowledging the traditional territory since March 2014. Due to conversations with Indigenous leaders, including the Aboriginal Advisory Committee as part of the 2018 Toronto for All Campaign, the language the City of Toronto uses has evolved.

Here are the types of scams we will be focusing on today...




These tend to be the most commonly used!

**Let's answer some
common questions!**




What are internet scams?

- Types of *fraud* that happen through the internet
 - Scams exist in different forms, for example:
 - Phishing emails
 - Phone calls
 - Text messages
 - And many more...
- 




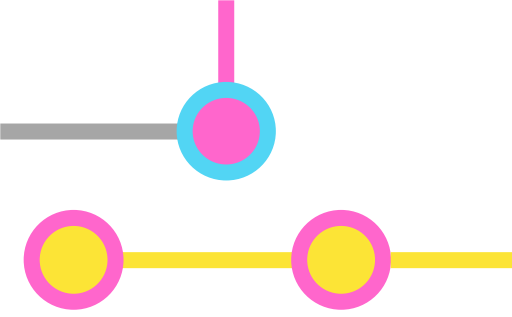
What does “phishing” mean?

- *Phishing* is the term used to refer to attempted attacks on your personal and private information
 - Typically, information such as credit card numbers, banking info, passwords, and identity info are primary targets
- 




Who is at risk?

- *Anyone* can be at risk, but...
 - Research has shown that older adults are among the most targeted groups of people
 - Reasons include:
 - Accumulation of assets
 - Decreased capacity/ willingness to report misbehavior
 - Health issues
 - Language barriers
- 




How do I know if I've been attacked?

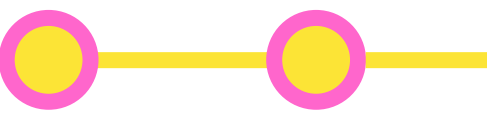
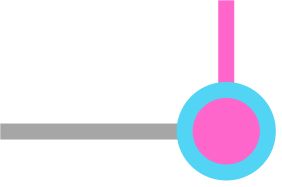
- Signs include:
 - Unusual activity on email or online bank accounts
 - Constant pop-ups on your screen and inability to close them
 - Random apps or software installed on your device without your consent or knowledge
 - Commonly used apps do not perform the same and have suspicious advertisements on them
 - Restricted access of own device
- 





What can I do to keep safe?

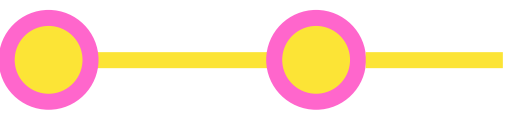
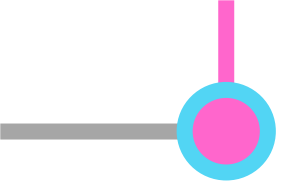
- We will look at some suggestions shortly
 - Some quick tips include:
 - Never share your passwords with anyone
 - Avoid clicking on random advertisements on the internet
 - Try not to do things like online banking in public areas
 - Keep your devices up-to-date
- 

Let's learn about
fake antivirus software!





What is antivirus software?

- 
- Antivirus software is a system that protects you from various threats to your computer
 - These can be purchased either directly from the developer or from verified retailers such as:
 - Best Buy
 - Walmart
 - The Source
 - Internet providers
- 



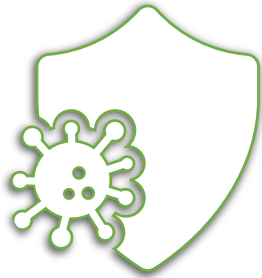
What is fake antivirus software?

- 
- These are systems *pretending* as legitimate protective options
 - They are marketed as free downloads on uncommon websites
 - They do not have any *recognizable branding* or manufacturer
- 

How to Identify Fake Antiviruses: *Tips & Tricks*



Advertised via an *alarming pop-up* (sudden message appearing) on your screen. Hard to close ad.



Message on your screen that reads *"device now infected"* by some *"dangerous threat"*.



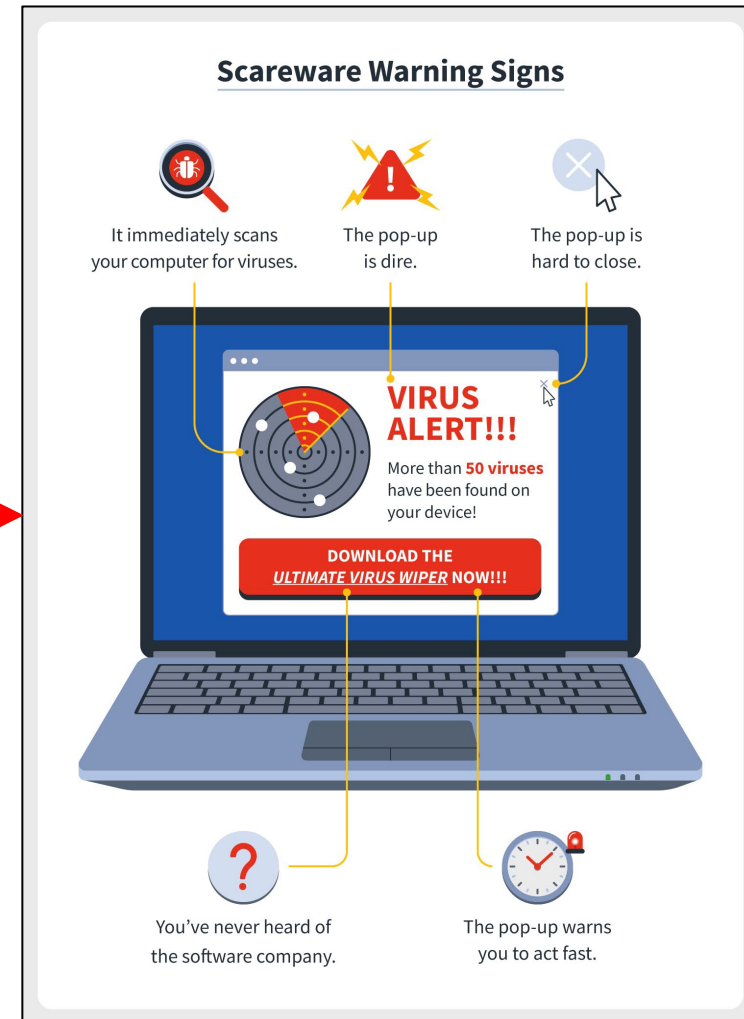
Told to take immediate action and **CLICK HERE** - or words to that effect



Once downloaded, usually *for free*, you get viruses, and other cyber threats

How to Identify Fake Antiviruses: *Example*


1. Message pop-up stating urgency of the matter
2. Immediate download of software without consent
3. Pop-up or message box is hard to close
4. Never heard of the company trying to install the software
5. Pretending to do a scan of your computer right away



Let's learn about
phishing emails!



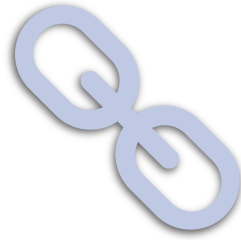
What is a “phishing email”?

- *Phishing emails* are emails that will often ask you for private, personal information
 - Sometimes these emails include links to unsafe websites or will attempt to pose as being sent from known companies like Rogers, Bell or even the government
- 

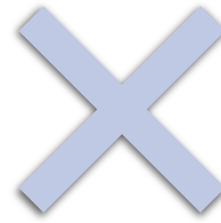
How to Identify Phishing Emails: *Tips & Tricks*



Being asked to *update bank or credit card* information on a fraudulent website



Suspicious *links or attachments* via email, social media or other messaging apps



Spelling or grammar mistakes – Fraudulent emails will usually have many spelling mistakes or irregularities in the email address



These emails will include *warnings or threats* in the main body of the email

How to Identify Fishing Emails: *Example*

1. Fake email - identified by irregularities
2. Threats of cancelling service or issues with account
3. Spelling and grammar mistakes found throughout
4. Email contains suspicious links or attachments
5. Pretending to do a scan of your computer right away

From: MSteam-Outlook Message Center <no-reply@office365protectionservices.co.uk>
Sent: 19 September 2018 11:44
To: Bob Smith <Bob.Smith@Company.com>
Subject: Account Verification

This mail is from a trusted sender.

Outlook

Threat
We're having trouble verifying your Office365 account: Bob.Smith@Company.com on our server, most features will be turned off.
To help prevent account malfunctions, please log into your account portal to verify your account.

Spelling mistakes

[SIGN IN TO MICROSOFT ACCOUNT PORTAL](#)

Note : Outlook will automatically fix your account after this process on the microsoft server and all account feautures will be turned back on

Thanks for using office365 , we hope to continue serving you.

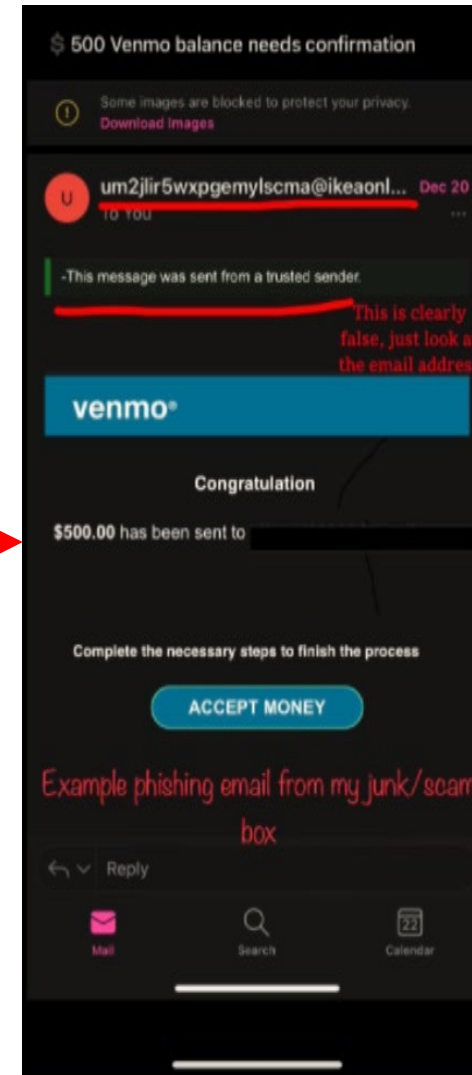
Microsoft Corporation
One-Microsoft Way Redmond
WA, 98052
All Right Reserved | Acceptable Use Policy | Privacy Notice

Grammatical errors

Fake email signature

How to Identify Phishing Emails: *Example # 2*



1. Suspicious subject line, relating to finances
2. Attempt at convincing you it is sent from a trusted source
3. Tempting you with fake financial or prize rewards
4. Buttons or links asking you to click on them
5. Email sorted into spam or junk folders



Let's learn about
technical support scams!



What is a “technical support scam”?

- 
- Sometimes appears as a message or pop-up on your device
 - Tells you your device is compromised and needs immediate attention
 - Accompanied by phone number to call or strange link to follow
- 

How to Identify Support Scams: *Tips & Tricks*



Browsing questionable websites will sometimes prompt you with these



The messages may ask you to call a random number or else something bad will happen to your pc

How to Identify Support Scams: *Tips & Tricks*



Ask you to give them **REMOTE ACCESS** to your computer



Pretend to run a **DIAGNOSTIC TEST**

How to Identify Support Scams: *Tips & Tricks*



Tell you they've 'discovered'
a VIRUS or other SECURITY issue



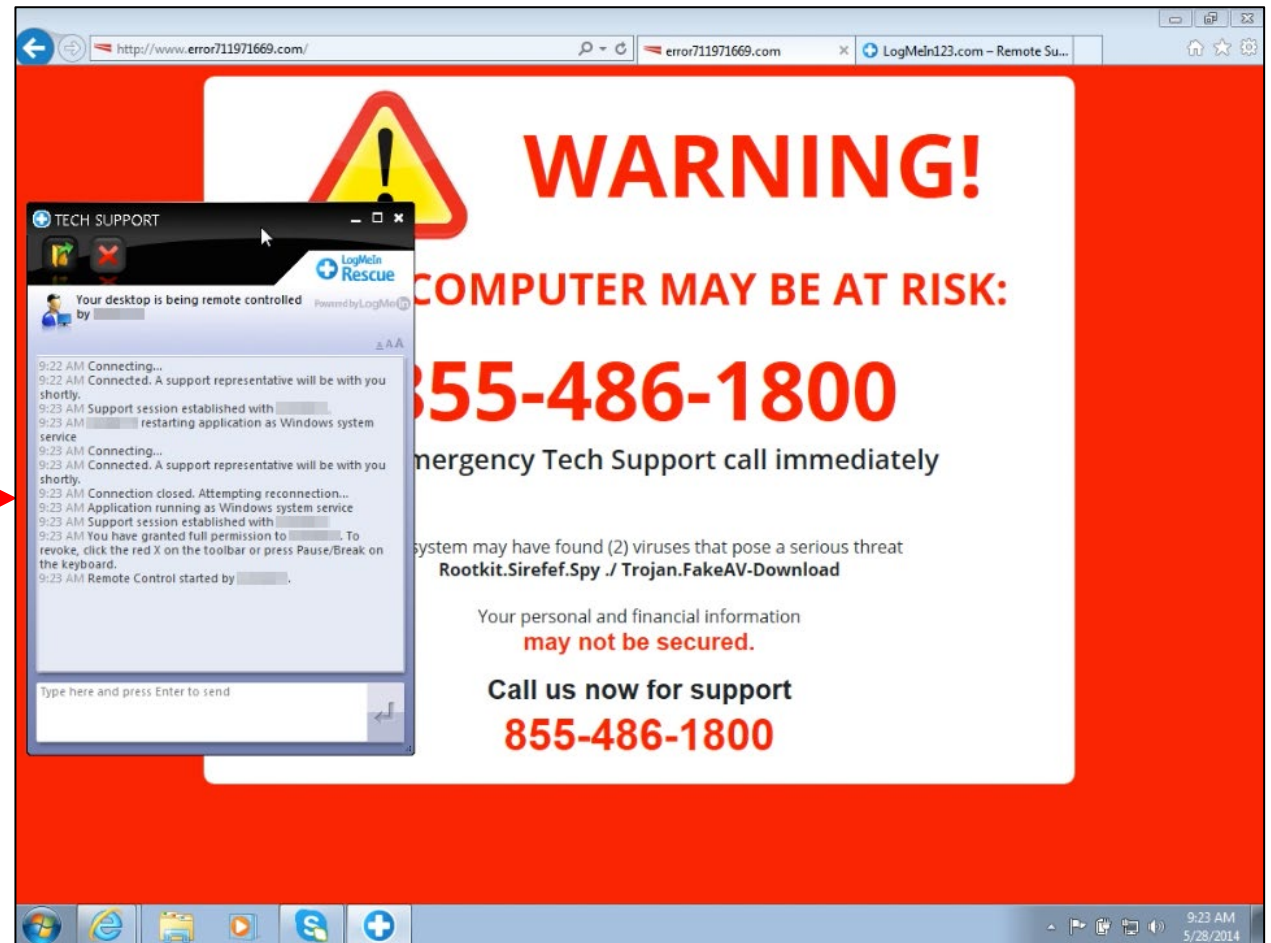
Try to sell you REPAIR SERVICES
or a SECURITY SUBSCRIPTION

THEN, YOU'RE ASKED TO **PAY A FEE.**

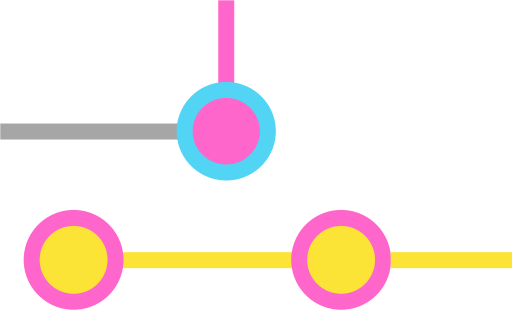
How to Identify Phishing Emails:

Example



1. New window or pop-up appears on your browser
2. Aggressive colors and flashing text
3. Random chat window opens with unknown "assistant"
4. Buttons or links asking you to click on them for security
5. Words like "trojan" or "virus" used to scare you



Let's learn about
phone scams!



What is a "phone scam"?

- 
- Attempts made by scammers and fraudulent companies over the phone to steal personal, banking, and other private information
 - Usually through the form of a phone call or text message
- 

How to Identify Scam Calls: *Tips & Tricks*



Caller ID shows caller to have a *strange area code* or phone *number similar* to yours



Caller ID may automatically let you know the call is "*suspected spam*"



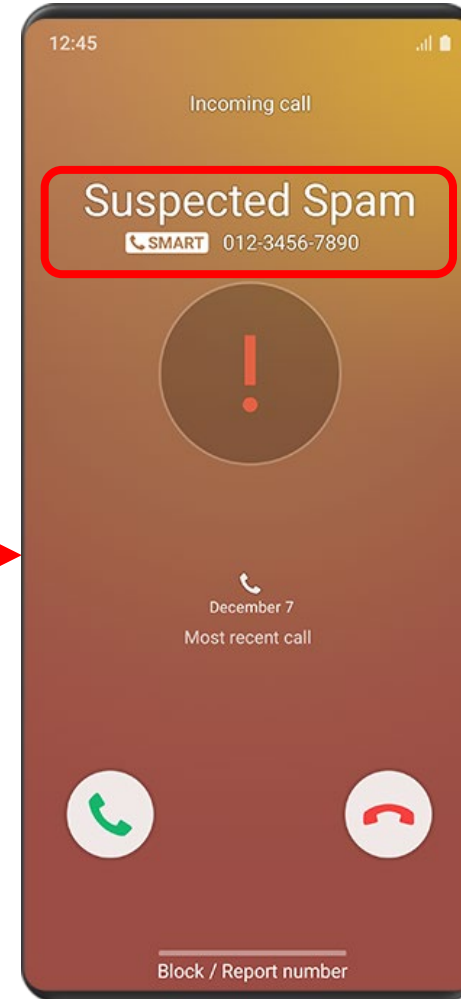
If you pickup, the caller may *pretend* to represent the police or government - *the real thing would never call you*



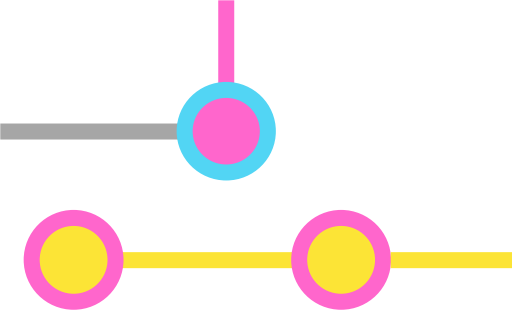
Aggressive language or *threats* are used to get you to provide information

How to Identify Scam Calls: *Example*



1. Phone number calling you seems suspicious
2. Caller ID labels it as potential spam or scam
3. Symbol or icon with an alert symbol to warn you



**Let's learn about
romance scams!**



What is a "romance scam"?

- 
- Criminals pretending to be interested in romantic partners on social media or dating websites
 - These scammers will take advantage of their "partner's" desire to find companionship in hopes of stealing money or other assets
- 

How to Identify Scam Calls:

Tips & Tricks

Their profiles have very few images or images that seem to be of models

Usually, they work or live in another country

Quickly ask you to talk on another messaging app

Professes love early on

Something always comes up when you plan to meet or video call

They request money from you relatively quickly



An example of a **romance scam**


<https://www.youtube.com/watch?v=0Gg-Bjvm7L8>

It's time for
an intermission!

**Let's define some more
important terms!**




Malware

- 
- General terms used for software that is meant to invade your devices and intentionally leak private information and gain access to secure systems






Ransomware

- A type of malware that will threaten to publish your private data or block access to your device unless a certain amount of money is paid
- 



Trojan

- A type of malware that misleads you into downloading it and installing harmful things on your computer
 - They pretend to be legitimate software and are sometimes difficult to distinguish from the real thing
- 

**How to
stay protected!**

How to Keep Safe from Viruses: *Tips & Tricks*



Stay aware of any random, unwanted pop-ups appearing on your screen - *close these as fast as possible*



Purchase and install a trusted antivirus platform through retailers like *Best Buy* or *The Source*

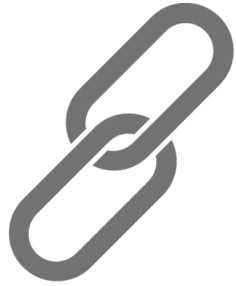


If your information has been compromised, *seek professional help immediately*



Never use the *same password* for multiple websites - *never share passwords* with anyone

How to Keep Safe from Viruses: *Tips & Tricks*



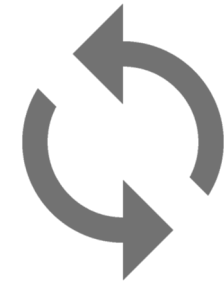
Don't click on
strange or
suspicious links



If possible, avoid
your email's *spam*
and junk folders -
fraudulent emails
will be filtered here



Don't answer calls
or texts from
numbers you *don't*
recognize - the
CRA will never text
or call you for
information



Keep your devices
up-to-date -
consistently check if
your phone, tablet,
or computer need
an update

Here are some popular, trusted antivirus platforms...



These are all available at Best Buy!

Note: Each provider has different versions that protect against different things



Ask about the differences in-store!

Keeping Safe

- Remember – close any suspicious windows or pop-ups
- Look out for grammar and spelling mistakes
- Never click unknown links or download random software
- In this example, the scammers are pretending to represent the government



http://mac-online-support.com

Are you sure you want to leave this page?

<http://fbi.gov.id657546456-3999456674.k8381.com>

YOUR BROWSER HAS BEEN LOCKED.

ALL PC DATA WILL BE DETAINED AND CRIMINAL PROCEDURES WILL BE INITIATED AGAINST YOU IF THE FINE WILL NOT BE PAID.

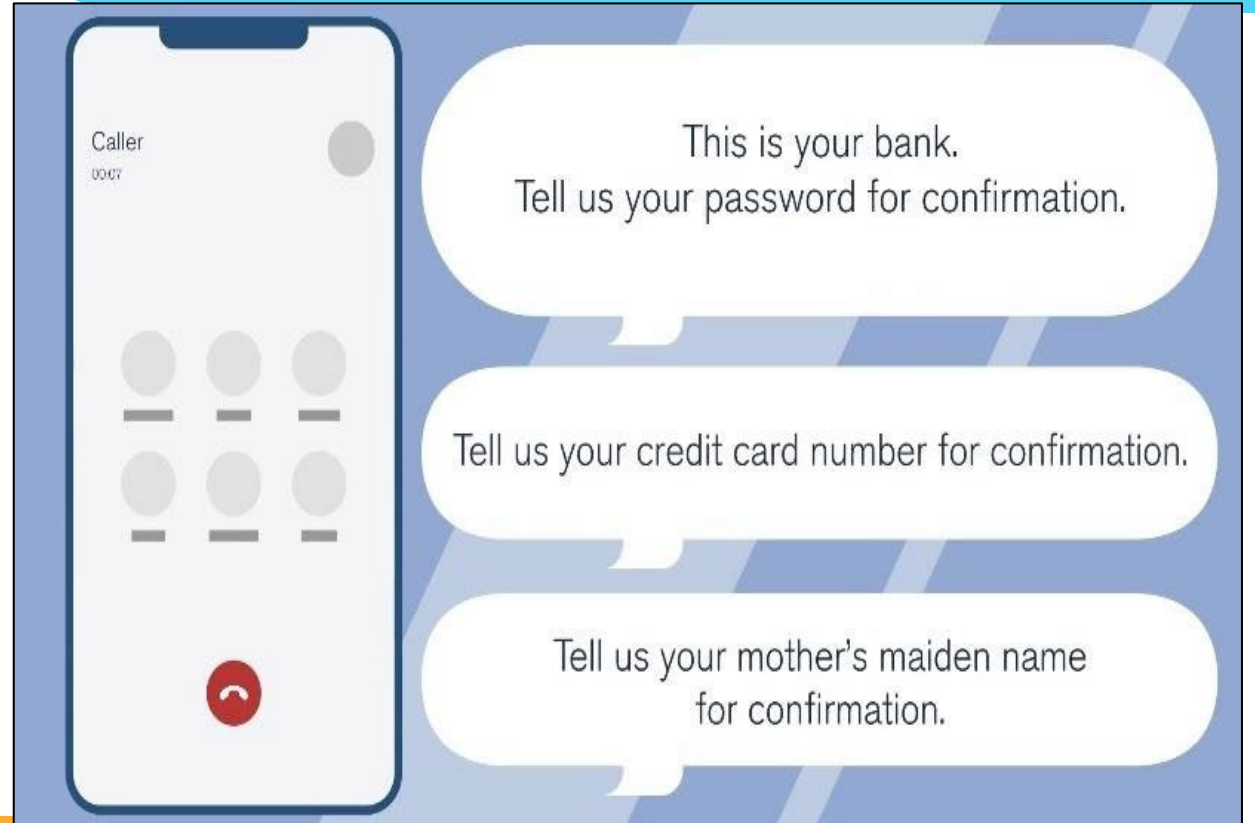
FOR HELP CALL TOLL FREE +1 800-798-8393

Stay on Page

Leave Page

Keeping Safe

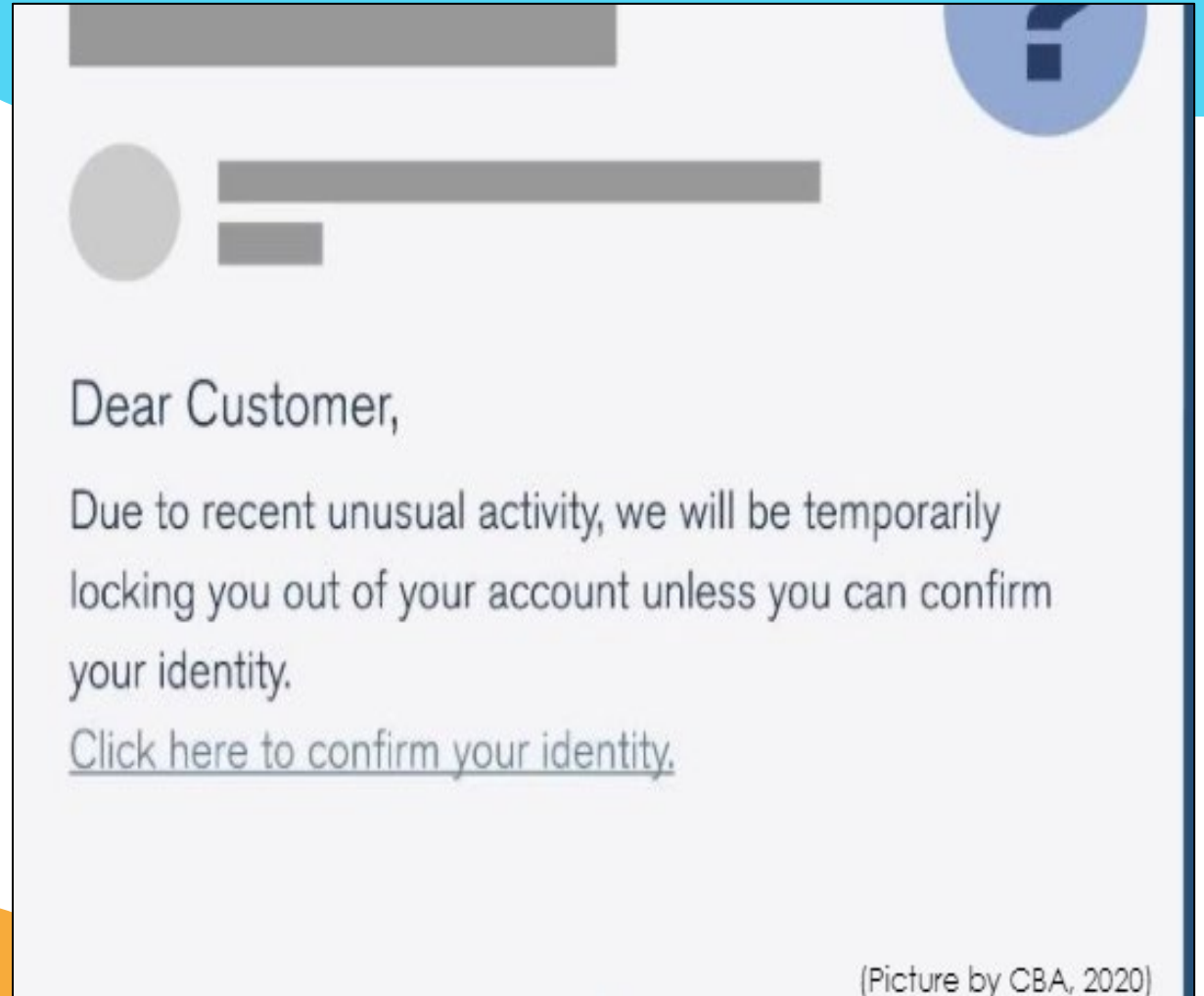
- Banking and government institutions *will never call you* to ask for personal information, unless you have personally dialed and are speaking to a legitimate representative
- Keep an eye on your caller ID – avoid *"SUSPECTED SPAM"* calls
- Ignore and robotic-sounding voicemails left by the caller



Note: fake CRA and police calls have been on the rise

Keeping Safe

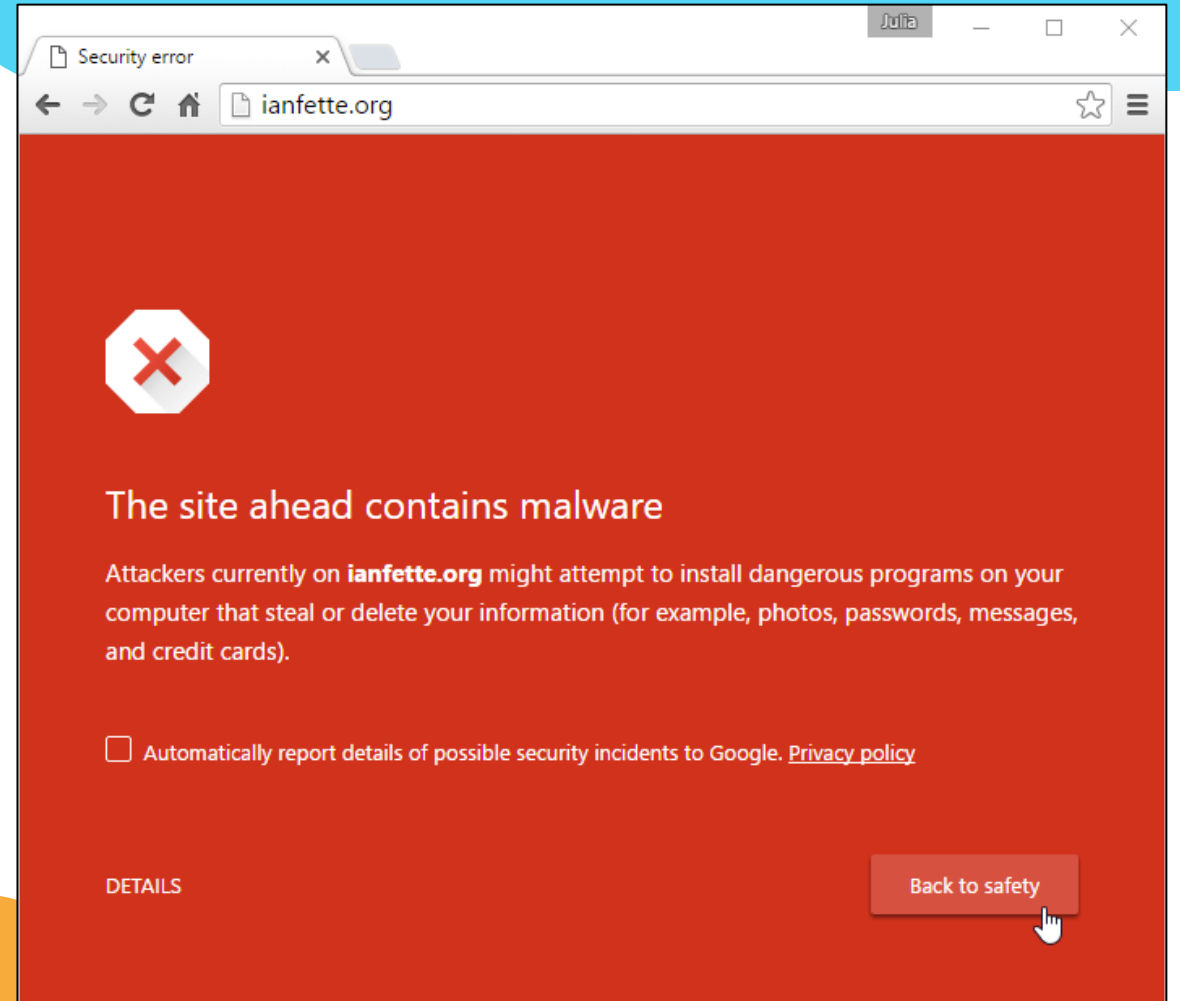
- Emails giving you warnings that your account is in danger can sometimes be legitimate
- Pay attention to the sender and subject line of the email - threats or warnings of restrictions placed on your account can be indicators of a potential scam
- Never click links without verifying the sender first



Note: if you received a message like this, manually change your password for that site and don't follow any links on the original email

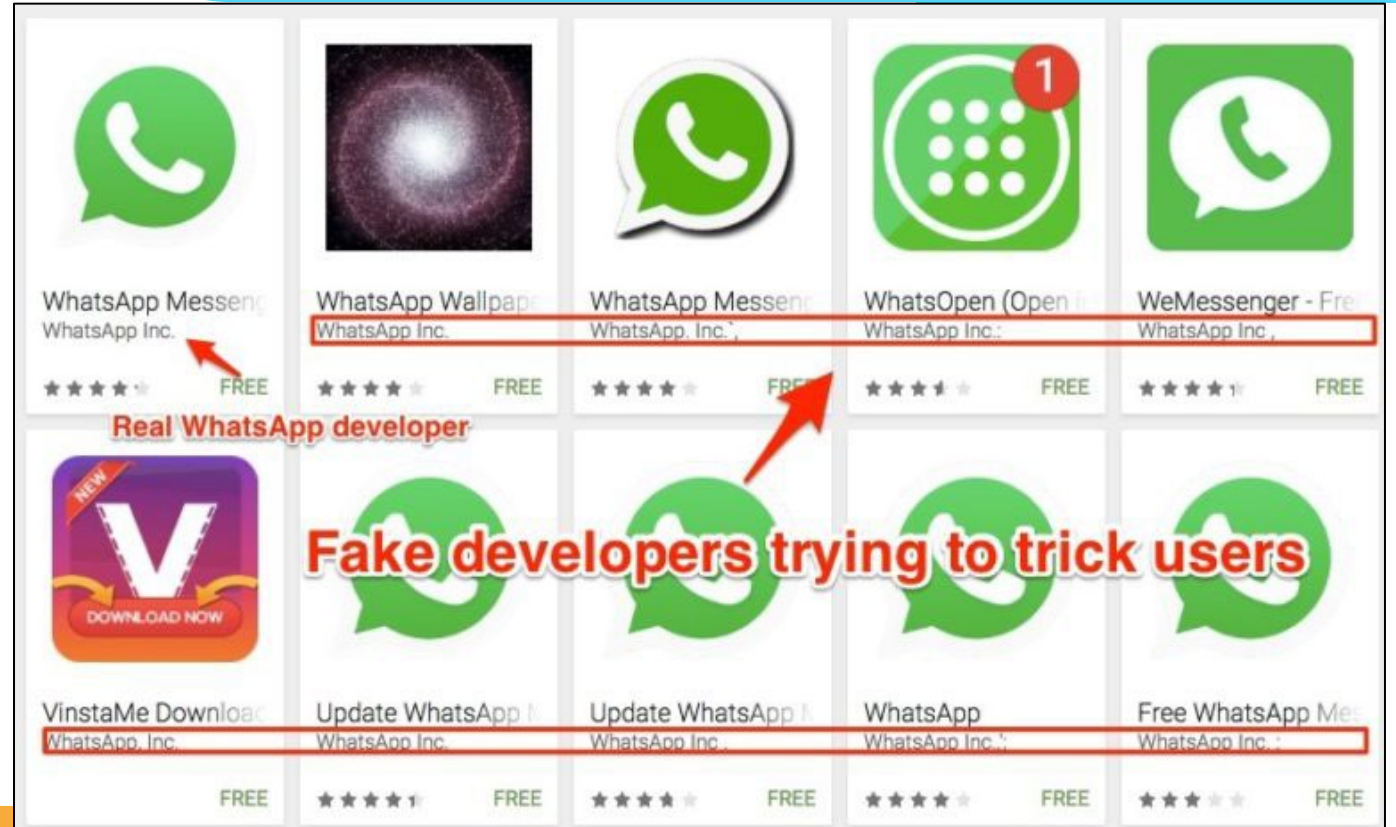
Keeping Safe

- Browsers like Google Chrome will offer free protection to a certain extent
- Google Chrome will warn you if the site you are visiting is potentially risky or unsafe
- If you ever see this while browsing, either close your browser right away or click *back to safety*



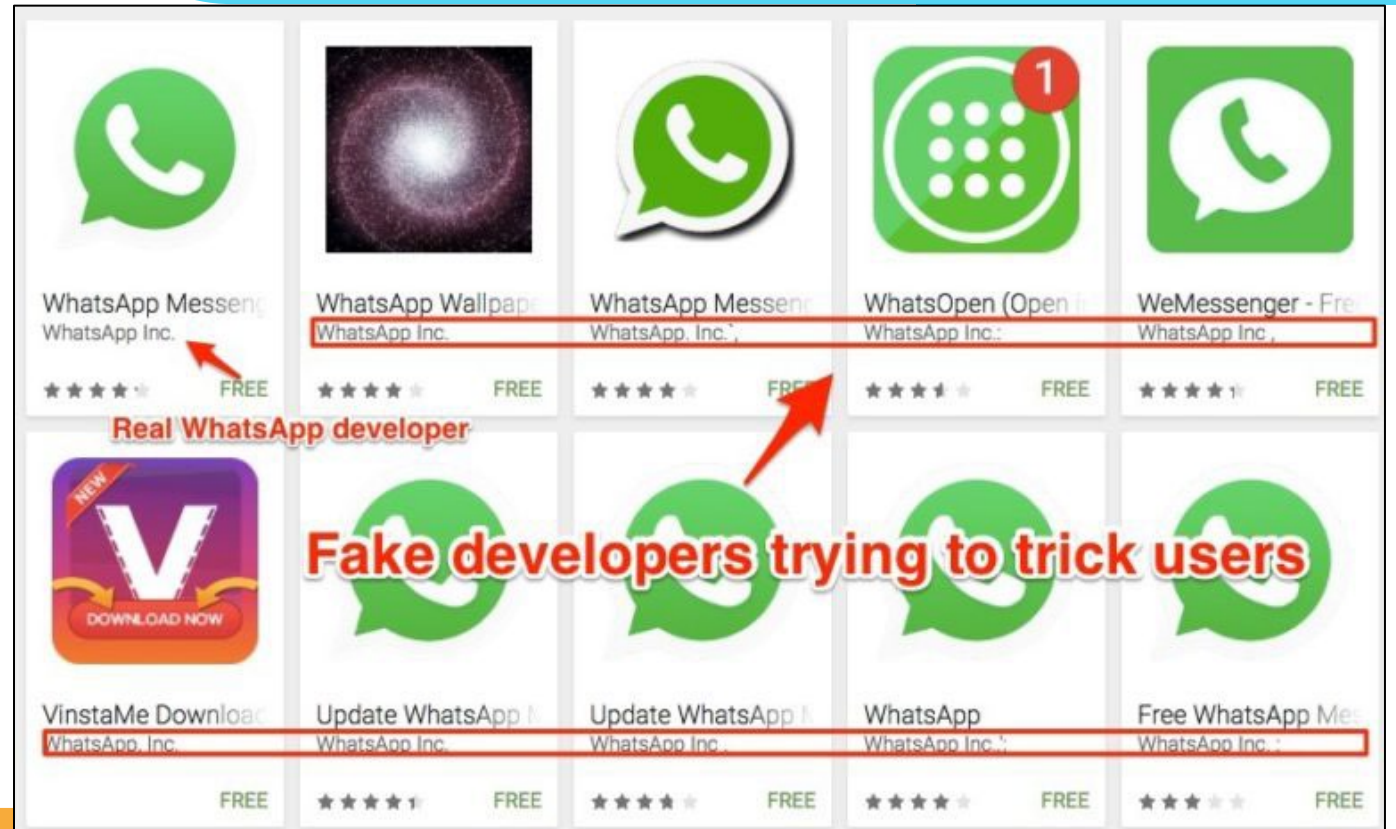
Keeping Safe

- Be wary of certain apps on your mobile phones or tablets
- Sometimes, there may be duplicate or similar looking apps on your app stores depending on what you are searching for
- Know the correct name of the developer before downloading



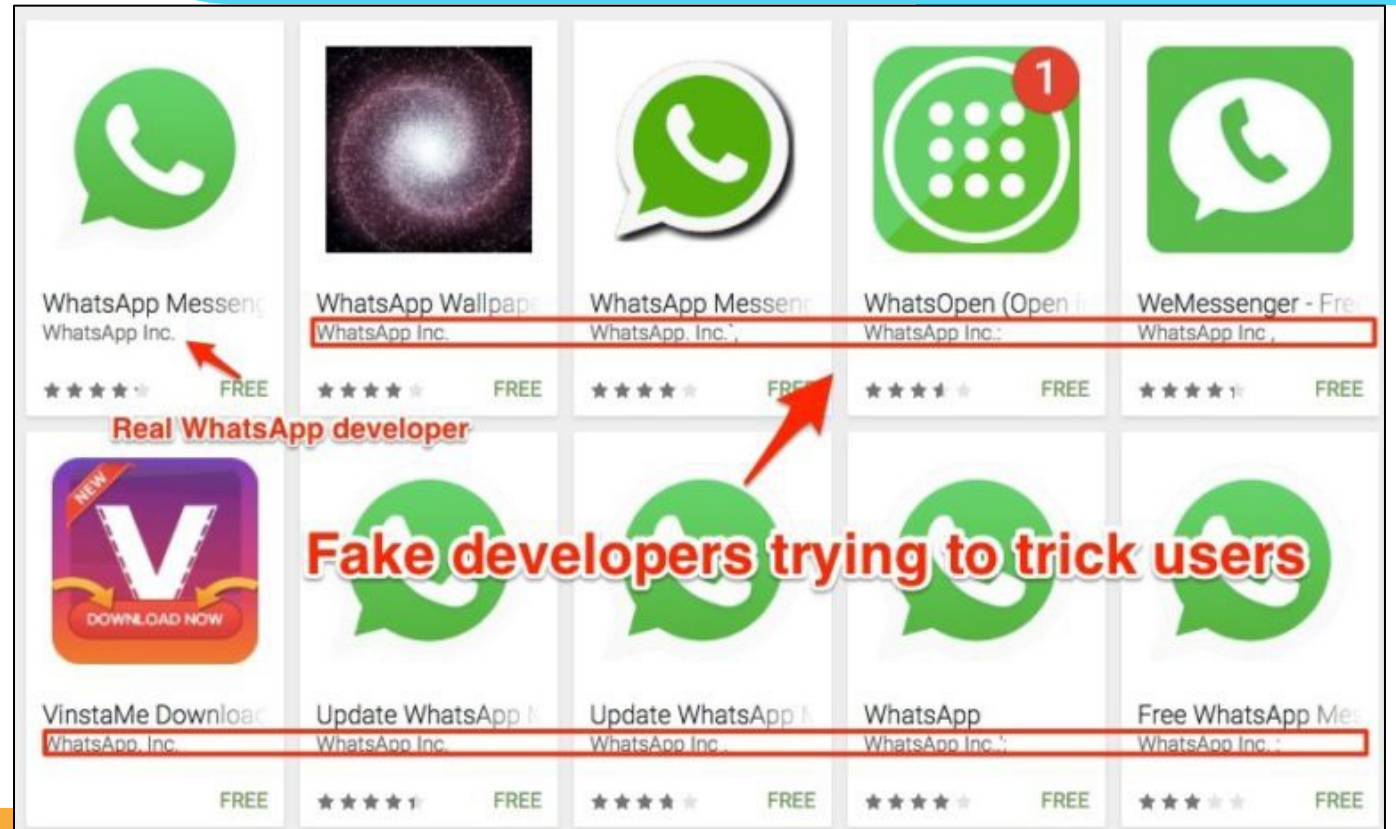
Keeping Safe

- The image to the right shows someone searching for WhatsApp, but there appear to be multiple apps made by different developers
- Typically, the first app to appear in your search results is the official and legitimate one people use



Keeping Safe

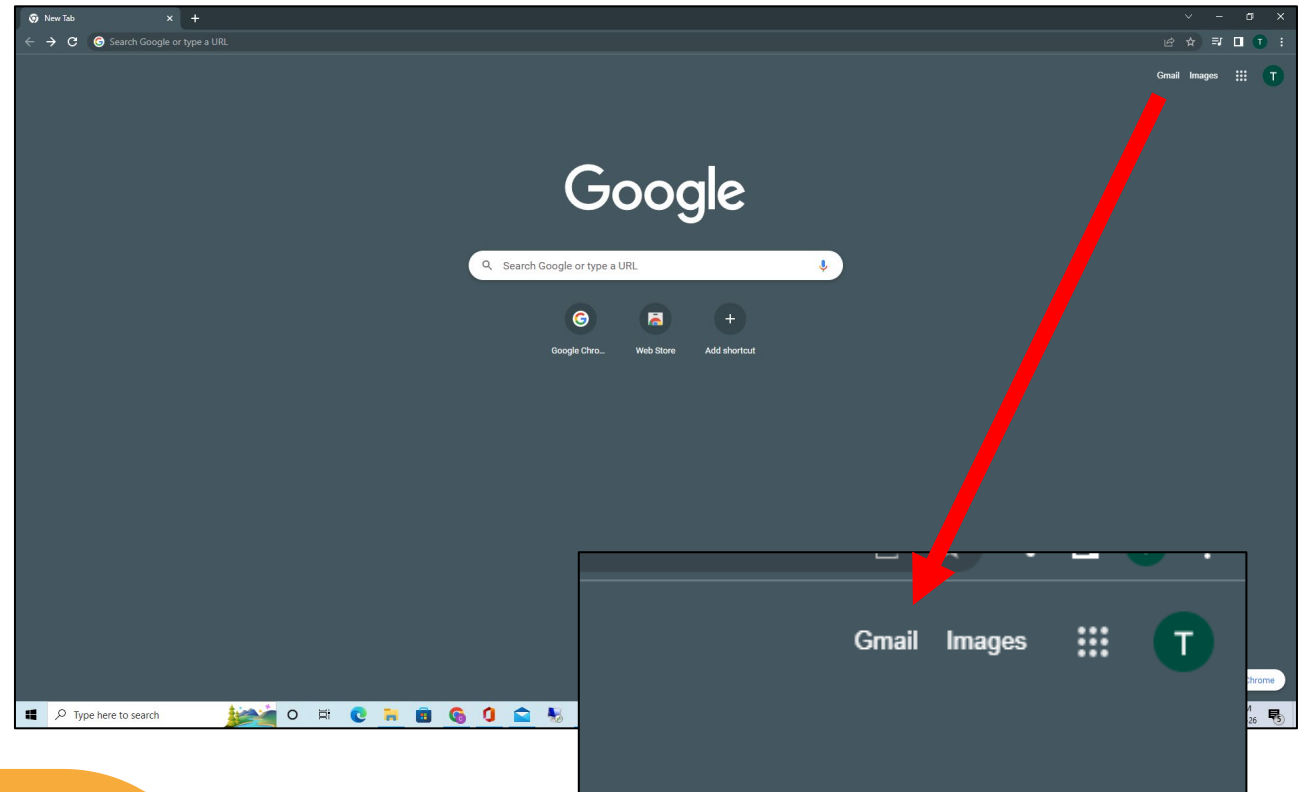
- Read the reviews on the app to ensure you are downloading something legitimate and without any major performance issues
- Typically, unsafe apps are rated very low and maintain 1-2 star ratings



How to block and report emails!

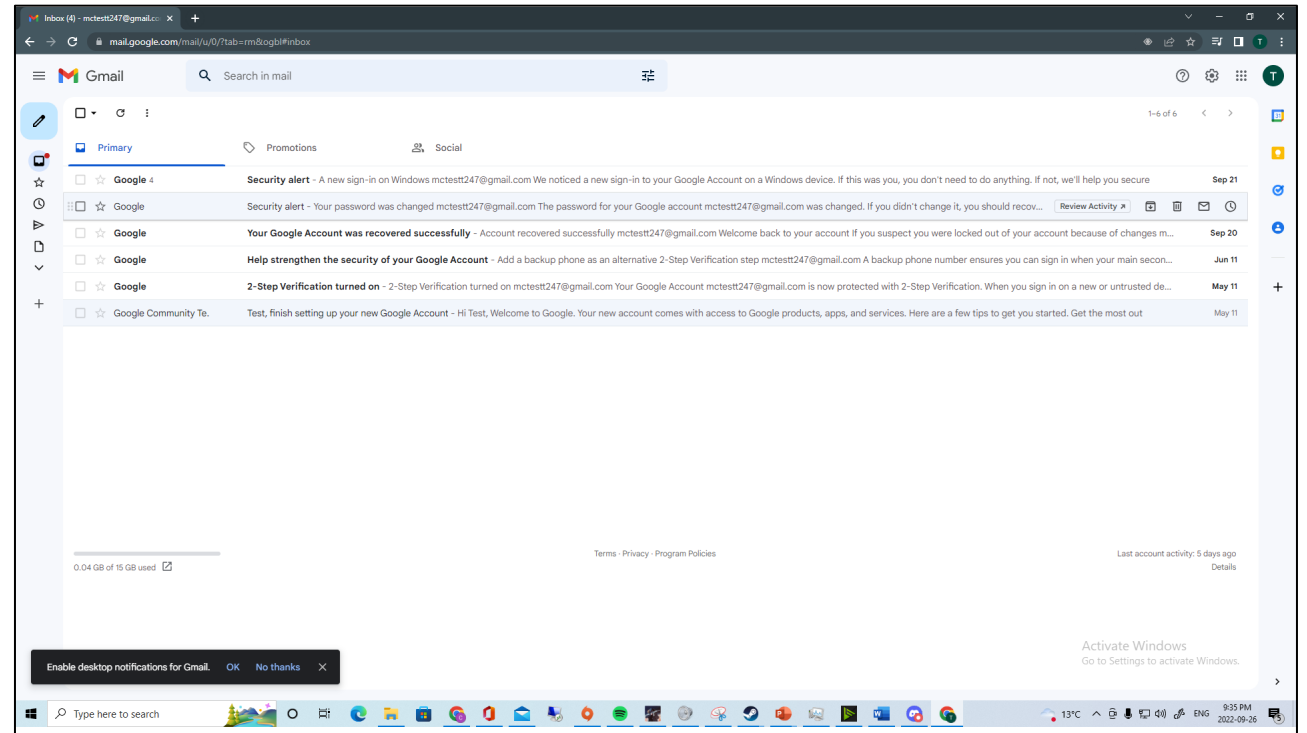
Keeping Safe

- Open Google Chrome - you can also use other internet browsers you prefer
- If you're using Chrome, click the Gmail button to sign-in to your Gmail account
- If you're using another browser, search for Gmail using your search bar



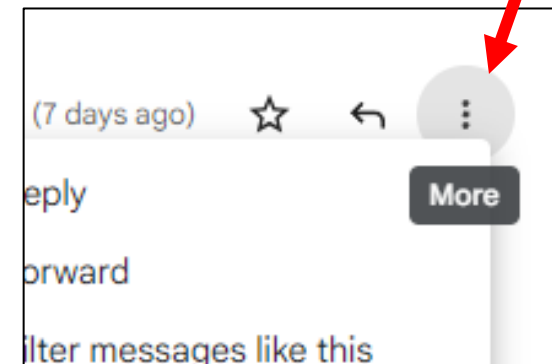
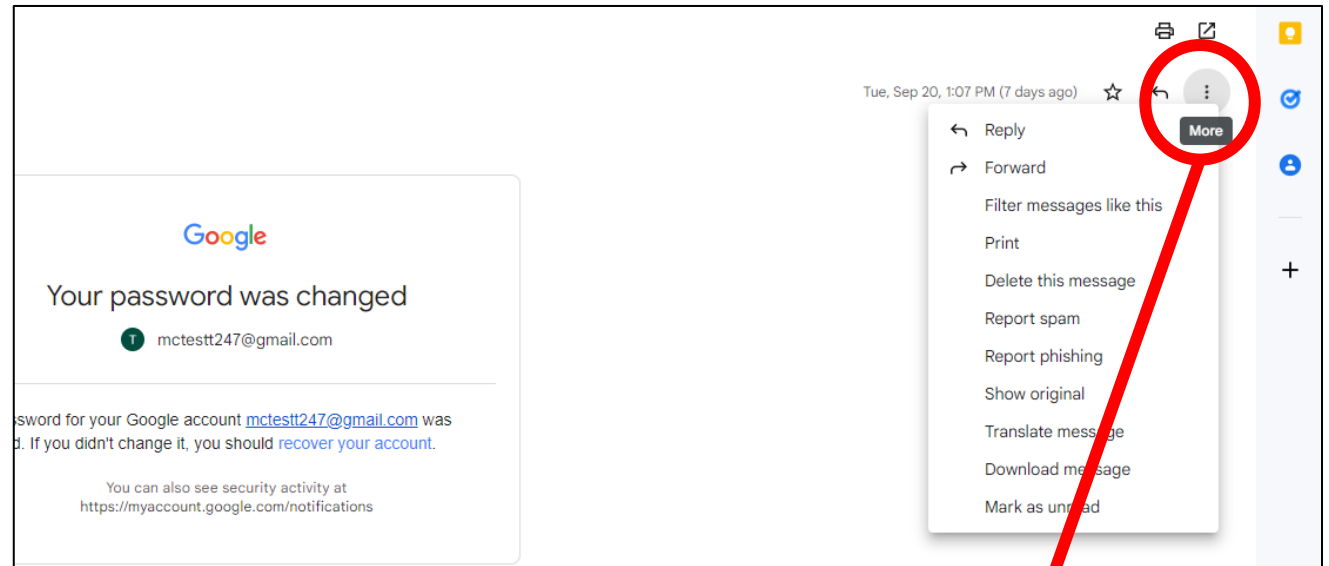
Keeping Safe

- Once signed-in, look for a non-important email that you may want to test the *report* feature on
- You can also look for something you think may be spam or junk
- Move your cursor overtop the email and left-click it once to select it



Keeping Safe

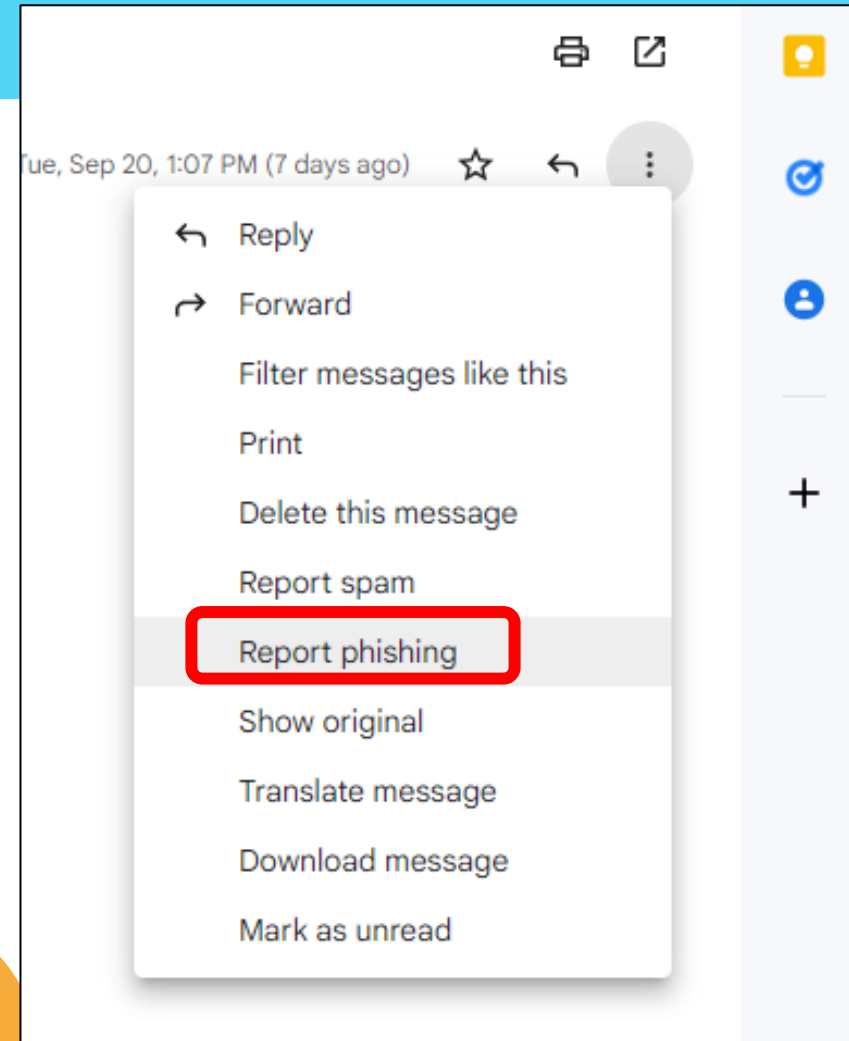
- Move your mouse to the right of the screen - find and left-click the 3 vertical dots
- Move your mouse to the right of the screen and find the 3 vertical dots
- Left-click the 3 dots (also called the *more* button) once to open a new menu



Note: hover your mouse over any icon or button to get its name or function

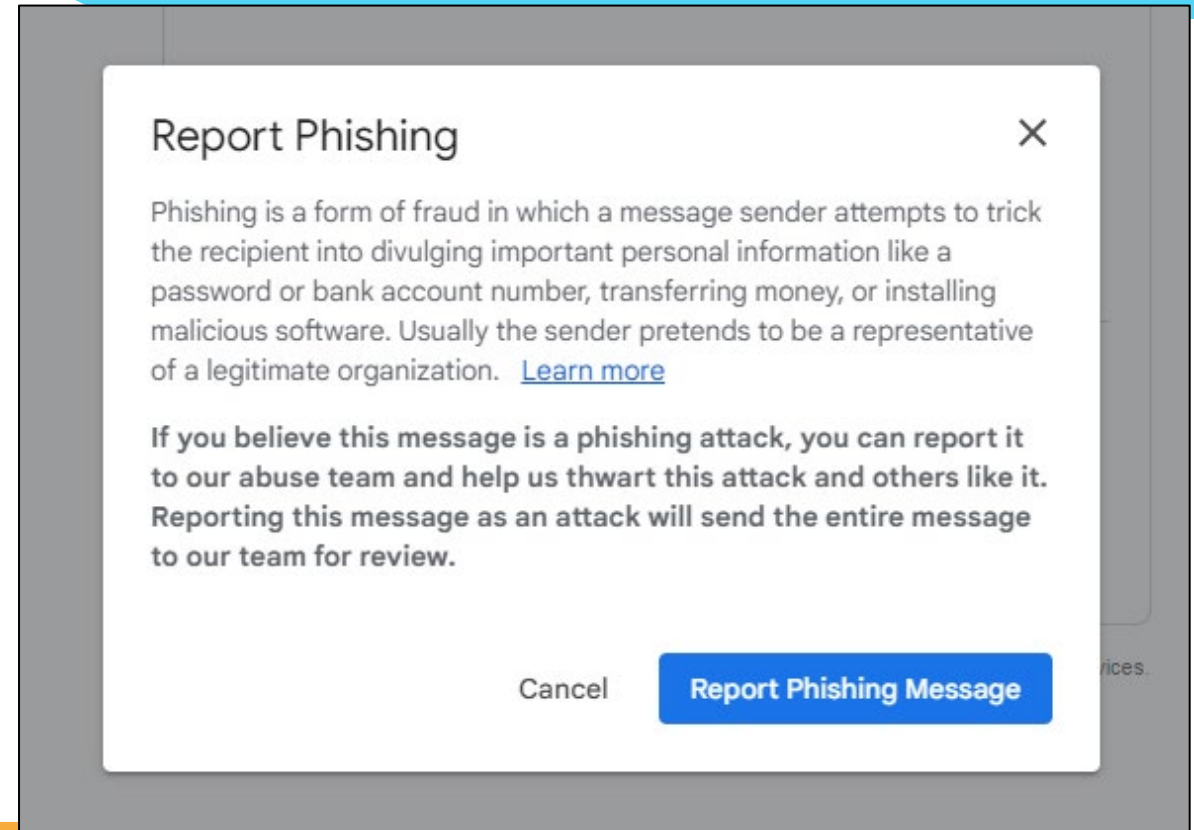
Keeping Safe

- In the new menu, you can either flag an email as *spam* or report it as *phishing*
- The spam option will only sort it and any future emails by the sender into the spam folder
- The phishing option will allow you to send the email to Google directly for review



Keeping Safe

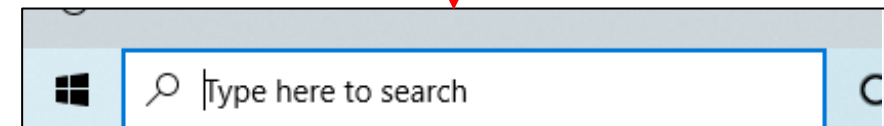
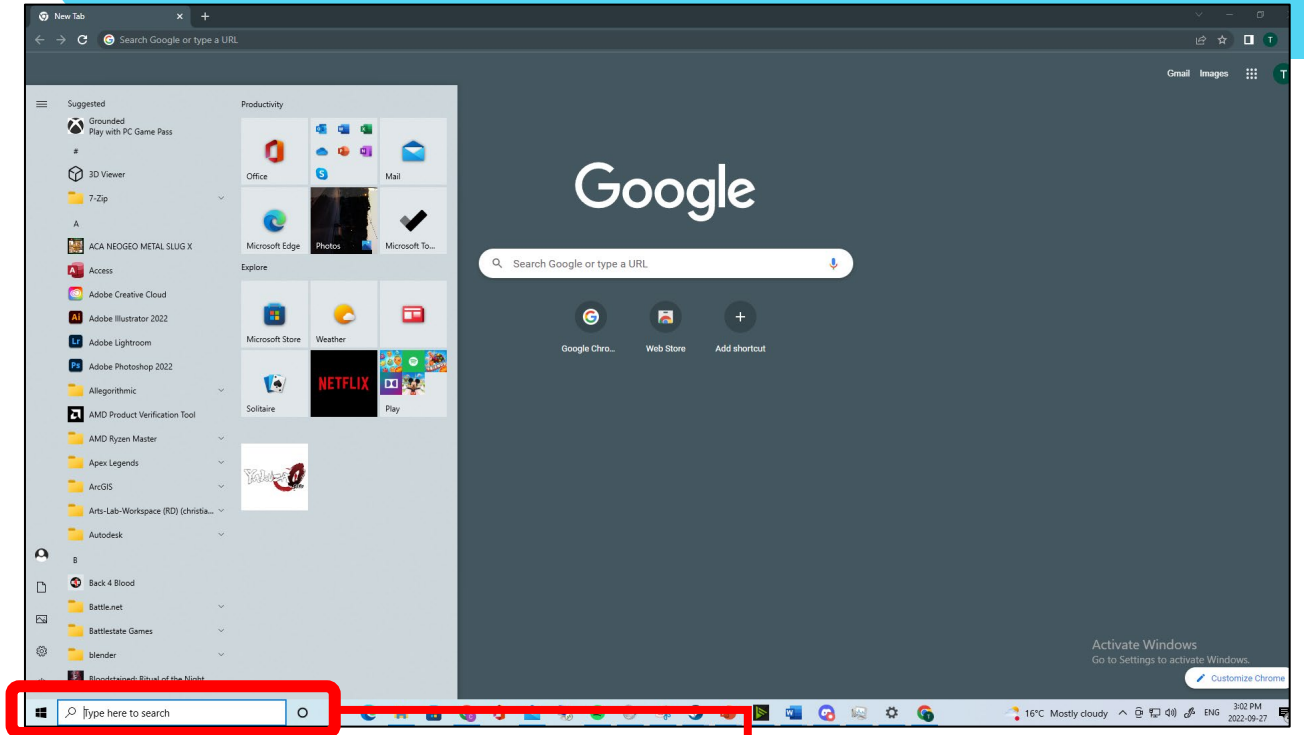
- If you've clicked the phishing option, you can finalize your report by clicking the *report phishing*
- It may take some time for Google to review the email and sender – at this point, you've done all you can



**How to
quickly check your computer!**

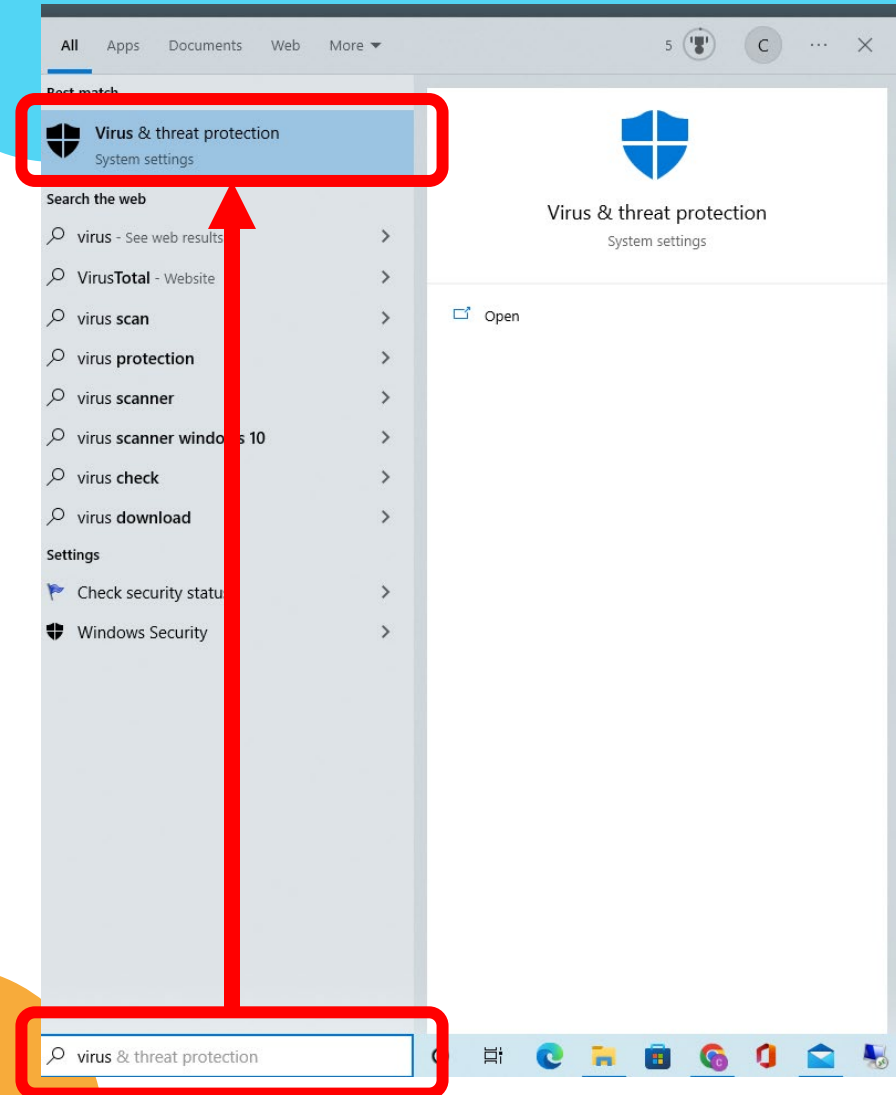
Keeping Safe

- Find and left-click the *Windows* button on the bottom-left of your screen
- This will open your *start menu* – from here you can search for and open different settings, apps, and operations on your computer



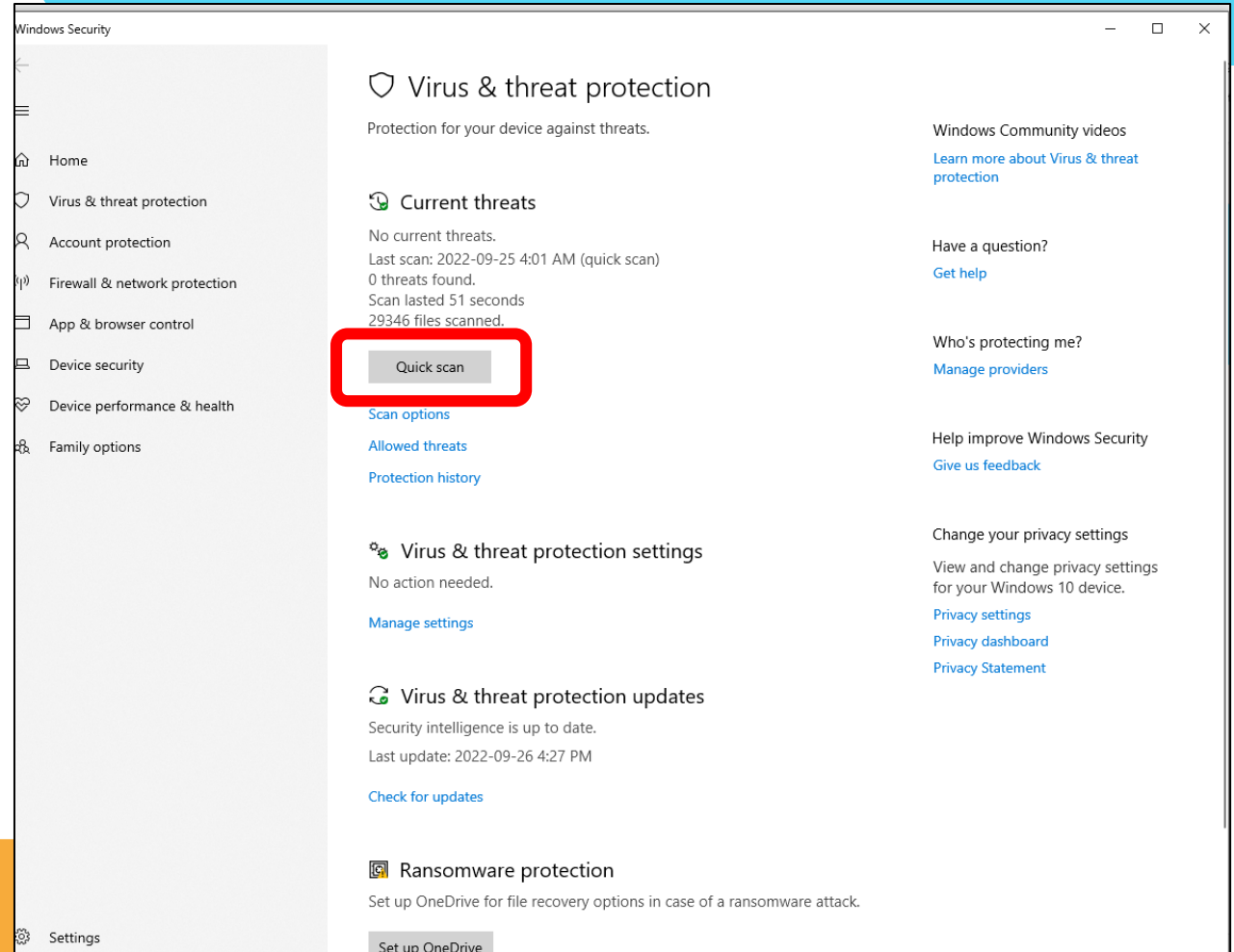
Keeping Safe

- In the *search bar* type "virus"
- You will notice an option called ***virus & threat protection*** will appear at the top of your search results
- Windows has a built-in, basic virus detection tool – left-click this option to open it



Keeping Safe

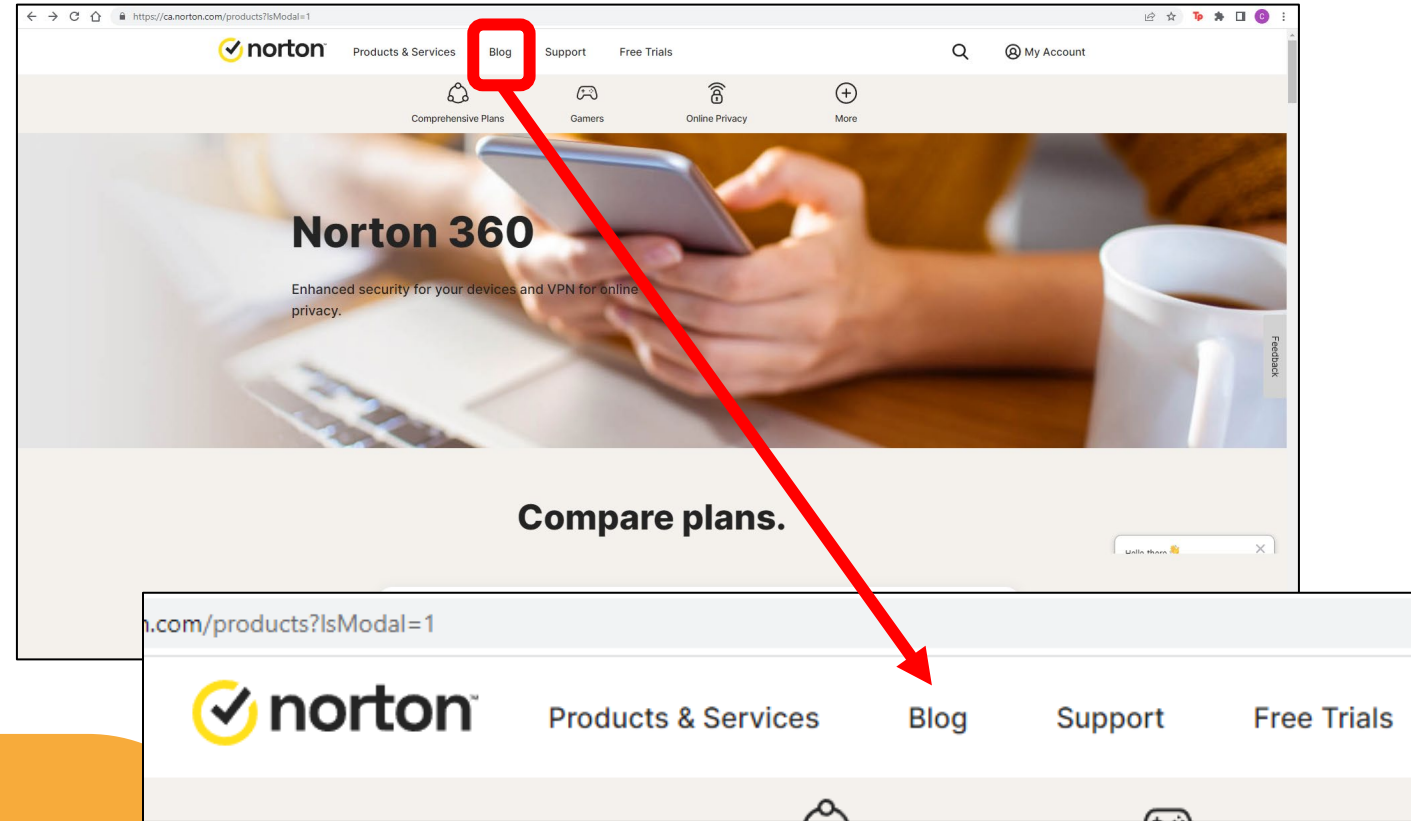
- This page will show you if there have been any threats detected and will give you an option to perform a **quick scan** on your computer
- You can click the quick scan button if you wish to ensure your device is safe



Let's look at some
extra resources!

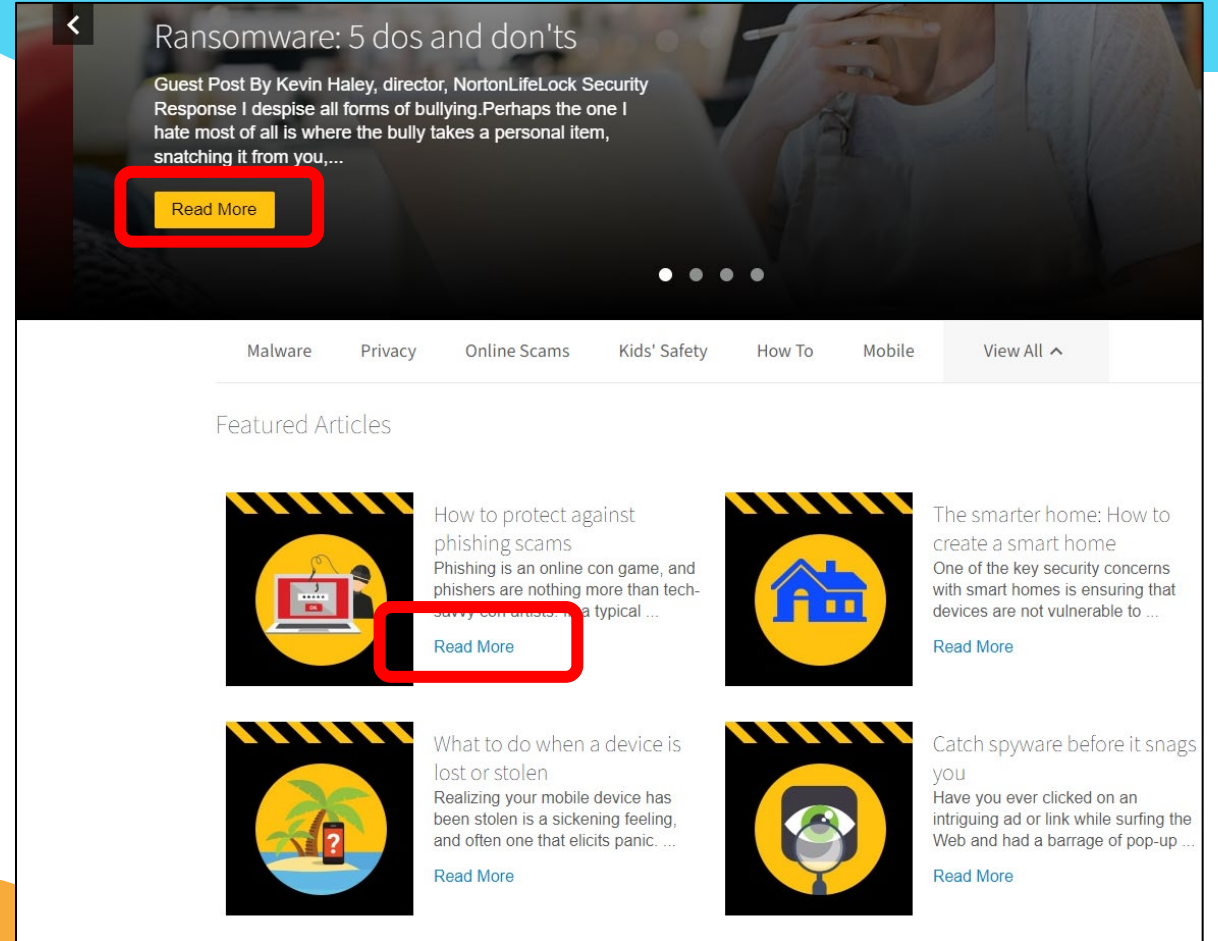
Keeping Safe

- You can also visit the website of antivirus providers such as Norton to get some additional information about how to stay safe
- In your browser, search <https://ca.norton.com> to access their website
- Click on the *blog* button at the top portion of the website



Keeping Safe

- The page that loads will give you a lot of in-depth information on the topics we've talked about today
- Click on *read more* on any of the articles listed to view the information



How to report emails in Outlook

<https://www.youtube.com/watch?v=0ttLtxIfPZQ>

How to **block emails in Yahoo Mail**

<https://www.youtube.com/watch?v=2wYE8fIAF1A>

How to check your iPhone for viruses

<https://www.youtube.com/watch?v=2ZPG--gGBQI>

How to check your Android for viruses

<https://www.youtube.com/watch?v=eEW0Pi89wyc>

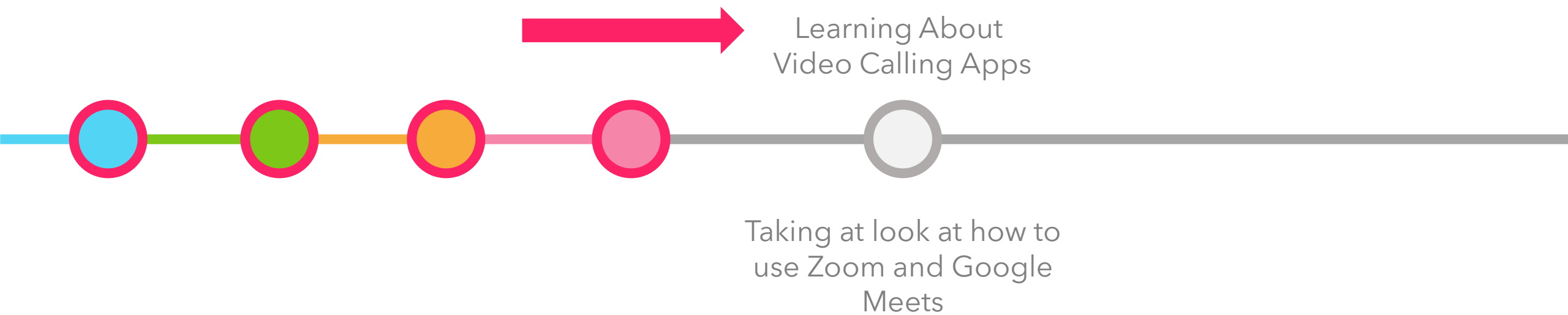
How to block numbers on iPhone

<https://www.youtube.com/watch?v=bHD2vYCsCFQ>

How to **block numbers on Android**

<https://www.youtube.com/watch?v=wWiRIMuxXXg>

Series Progress



That's it for now!
Any Questions?

