PHISHING LECTURE

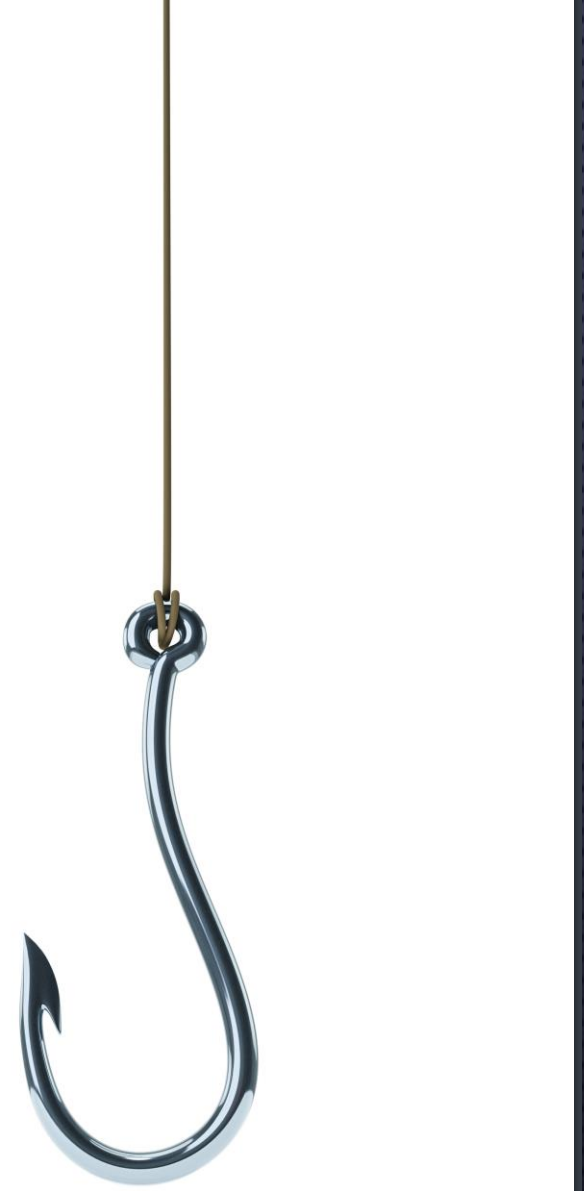
Ravindra Das

Harper College

HELLO, AND WELCOME TO THIS COURSE. IN THIS CLASS, WE WILL REVIEW WHAT PHISHING IS ALL ABOUT, AND HOW TO MITIGATE THE RISK FROM YOU BECOMING A VICTIM. ALSO, WE WILL DISCOVER HOW GENERATIVE AI IS NOW, UNFORTUNATELY, BEING USED BY THE CYBERATTACKER, IN ORDER TO CRAFT EVEN MORE CONVINCING, MALICIOUS EMAILS.

YOU WILL BE ASSIGNED A LETTER GRADE IN THIS CLASS; THE GRADE YOU WILL RECEIVE WILL DEPEND UPON HOW MUCH YOU PARTICIPATE. PARTICIPATION ALSO INCLUDES ASKING QUESTIONS IN THE CHAT WINDOW.

THIS COURSE IS DESIGNED TO BE IN AN OPEN FORMAT, AND IF YOU HAVE ANY QUESTIONS (WHICH IS AGAIN, VERY HIGHLY RECOMMENDED), PLEASE DON'T HESITATE TO ASK. I WILL ALSO BE AVAILABLE FOR HELP EVEN AFTER THIS CLASS IS OVER. THE SYLLABUS HAS MY CONTACT INFORMATION.

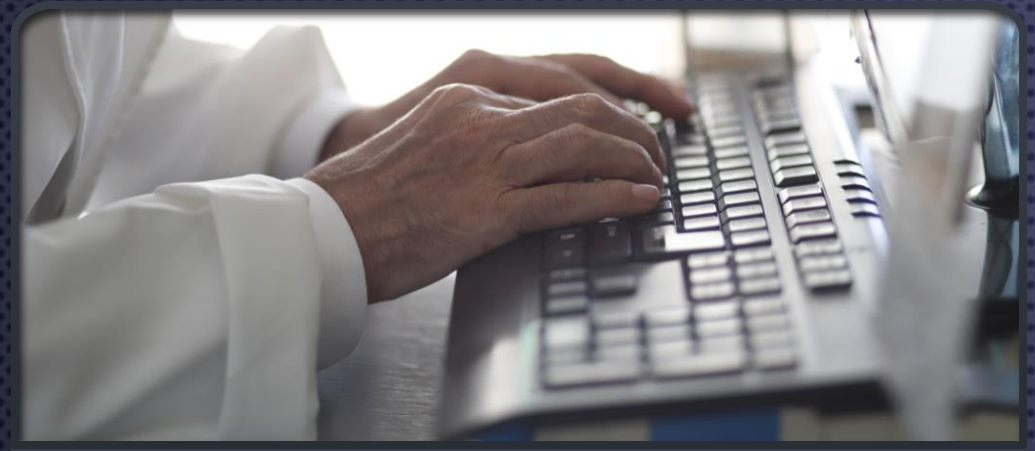


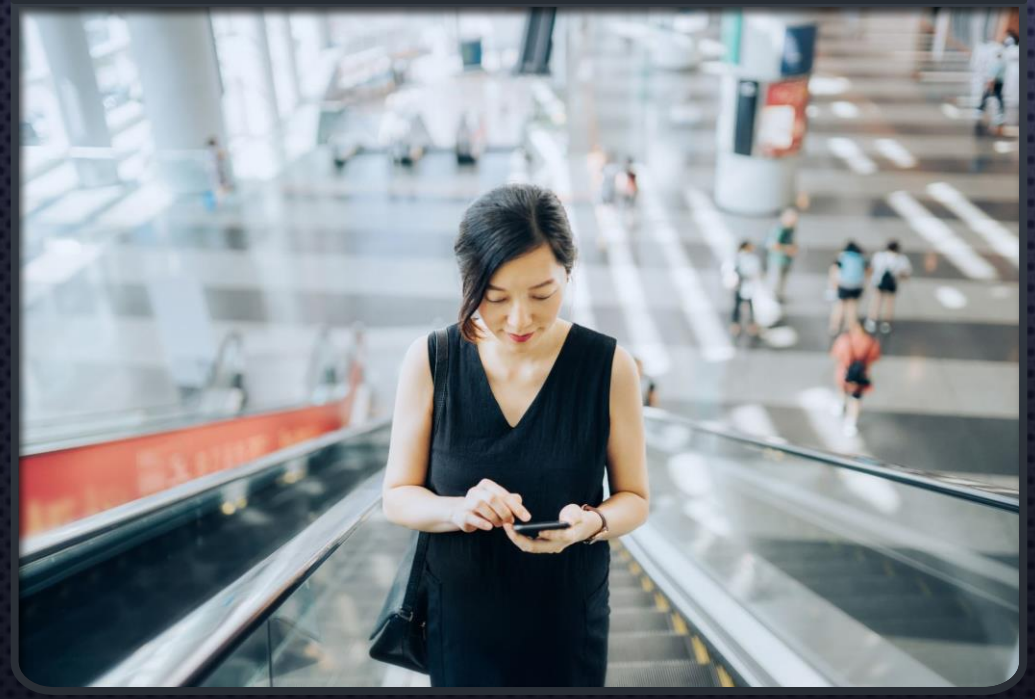
WHILE MOST OF US HAVE HEARD OF PHISHING TO SOME DEGREE OR ANOTHER, SOME OF US MAY NOT HAVE HEARD OF IT BEFORE. THEREFORE, A DEFINITION OF IT IS AS FOLLOWS:

> "PHISHING IS THE PRACTICE OF SENDING FRAUDULENT COMMUNICATIONS THAT APPEAR TO COME FROM A LEGITIMATE AND REPUTABLE SOURCE, USUALLY THROUGH EMAIL."

SOURCE: HTTPS://WWW.CISCO.COM/C/EN/US/PRODUCTS/SECURITY/EMAIL-SECURITY/WHAT-IS-PHISHING.HTML

IN OTHER WORDS, YOU ARE RECEIVING AN EMAIL MESSAGE THAT LOOKS LEGITIMATE, BUT IS ACTUALLY SPOOFED, IN ORDER TO TRICK YOU INTO SUBMITTING YOUR CONFIDENTIAL AND PRIVATE INFORMATION. FROM HERE, THESE CAN THEN BE USED TO LAUNCH COVERT AND EVEN MORE MALICIOUS ATTACKS, SUCH AS THAT OF IDENTITY THEFT.





ALTHOUGH PHISHING IS ONE OF THE MOST COMMONLY USED THREAT VECTORS OF TODAY, IT IS STILL ACTUALLY QUITE OLD, HAVING ITS FIRST ORIGINS BACK IN THE EARLY 1990S.

1990s

The 1990s: The first attack came onto AOL, in which millions of subscribers were impacted.

1996

The term Phishing became official, which was created by a group called "AOHell".

2001

Phishing groups start to create spoofed websites, impersonating PayPal and eBay.

2004

Pop windows start appearing in web browsers.

2008

Bitcoin launched, and Phishing attacks spike, causing almost $930 million in damages.

Harper College

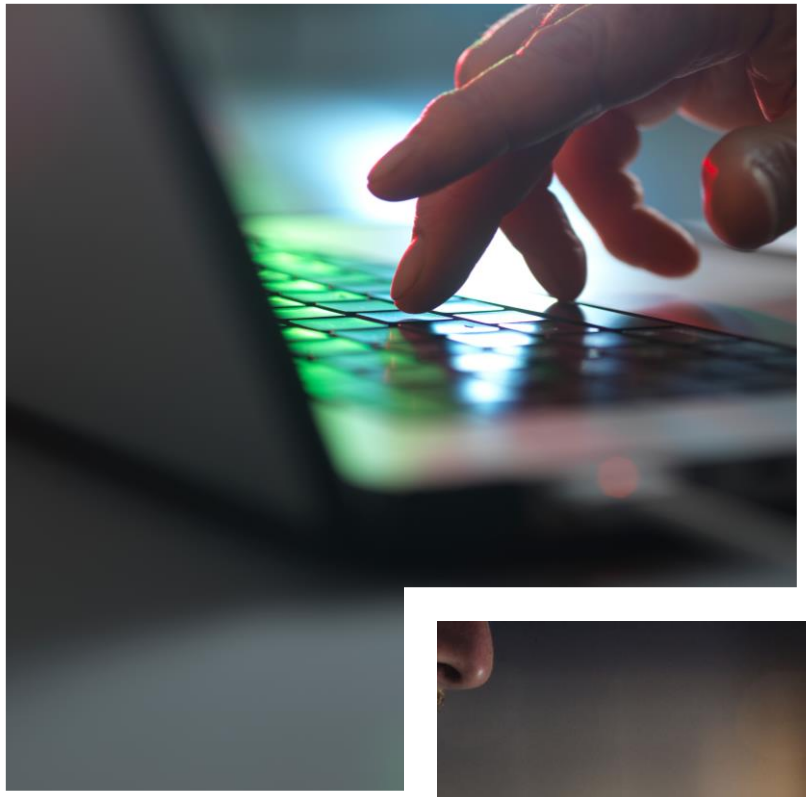
THE HISTORY OF PHISHING, CONTINUED:

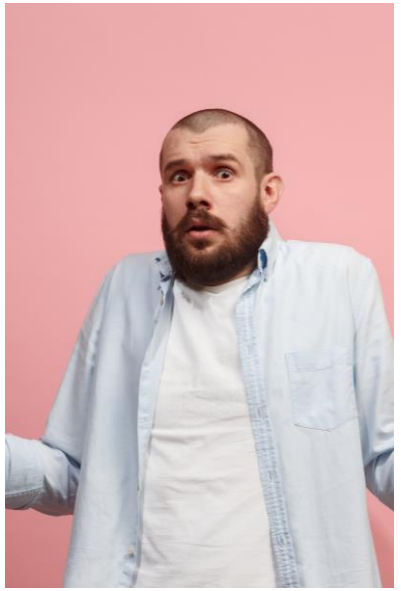
SOURCE: https://www.getcybersafe.gc.ca/en/resources/history-phishing)

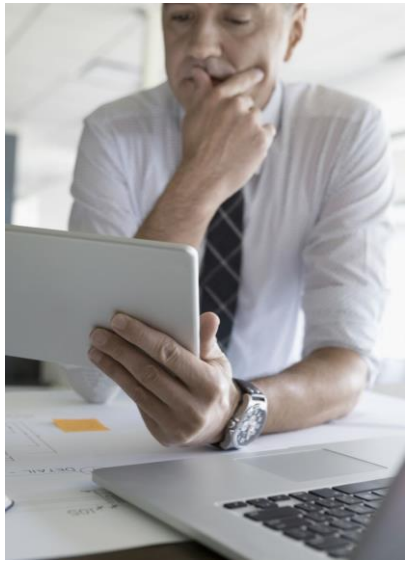
THE "TRADITIONAL" NUANCES OF A PHISHING EMAIL INCLUDE THE FOLLOWING:

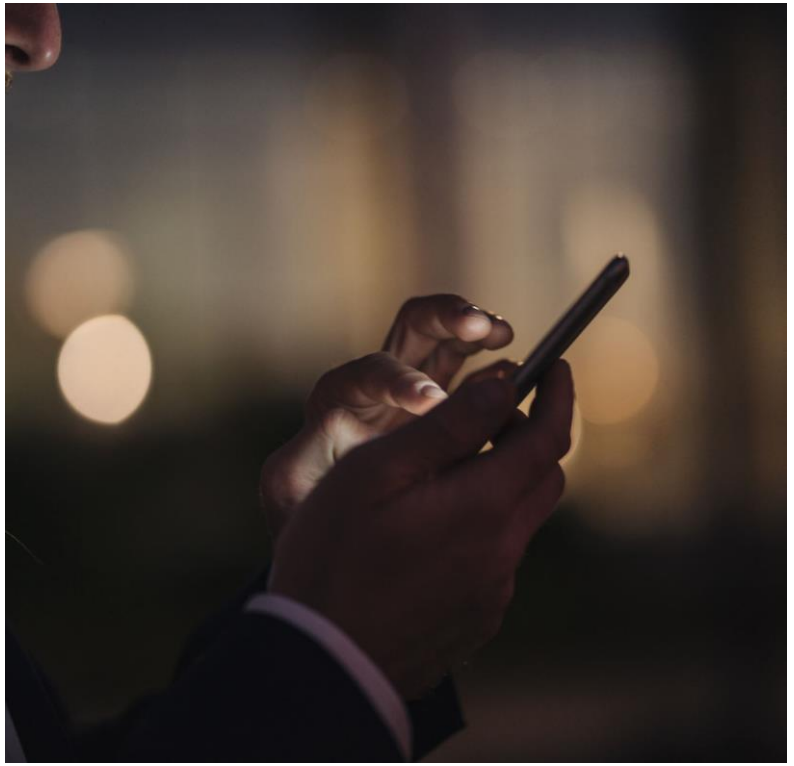
- **UNRECOGNIZABLE SENDER:** THIS IS WHERE YOU SIMPLY CANNOT RECOGNIZE THE SENDER OF THE EMAIL. EVEN SEARCHING IN GOOGLE DOES NOT YIELD ANY TANGIBLE RESULTS.
- **OFF SUBJECT LINE:** VERY OFTEN, THE SUBJECT OF THE EMAIL WILL LOOK STRANGE AT FIRST GLANCE.
- **DIFFERENT REPLY-TO ADDRESS:** WHEN YOU GET AN EMAIL, YOU CAN NORMALLY SEE THE EMAIL ADDRESS OF THE SENDER. AND, WHEN YOU HIT REPLY, THIS EMAIL SHOULD STILL BE THE SAME. BUT IN A PHISHING EMAIL, THE REPLY-TO ADDRESS WILL BE COMPLETELY DIFFERENT.

Harper College





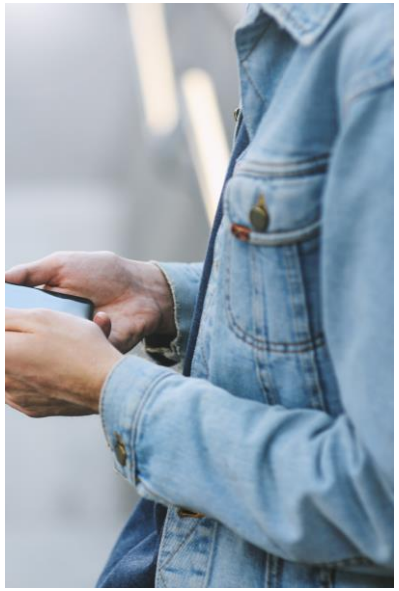




THE "TRADITIONAL" NUANCES OF A PHISHING EMAIL INCLUDE THE FOLLOWING, CONTINUED:

- **Misspellings:** This was one of the most obvious clues to a phishing email. However, with generative AI today, especially that of ChatGPT, this is no longer the case.
- **Mismatch in the links:** Most phishing emails will have some sort of URL in them for you to click on. But when you hover your mouse over it, a different URL will appear.
- **A sense of urgency:** Most phishing emails will have a sense of urgency for you to act quickly.

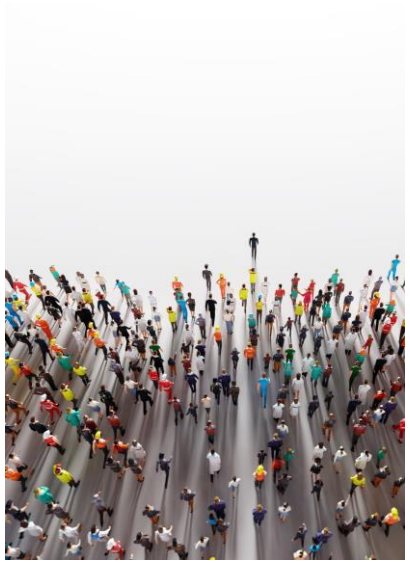
Harper College

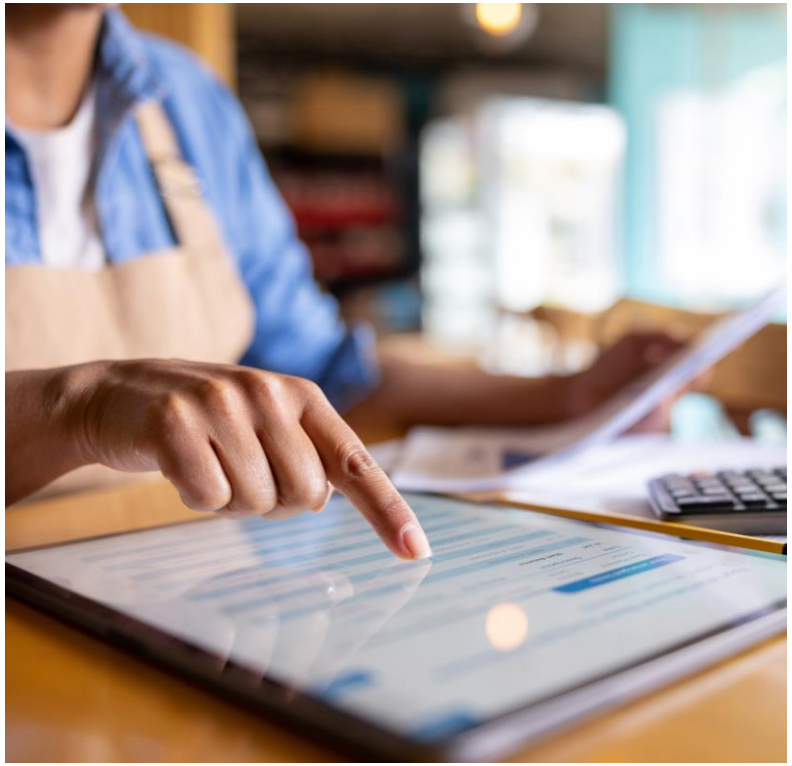


THE "TRADITIONAL" NUANCES OF A PHISHING EMAIL INCLUDE THE FOLLOWING, CONTINUED:

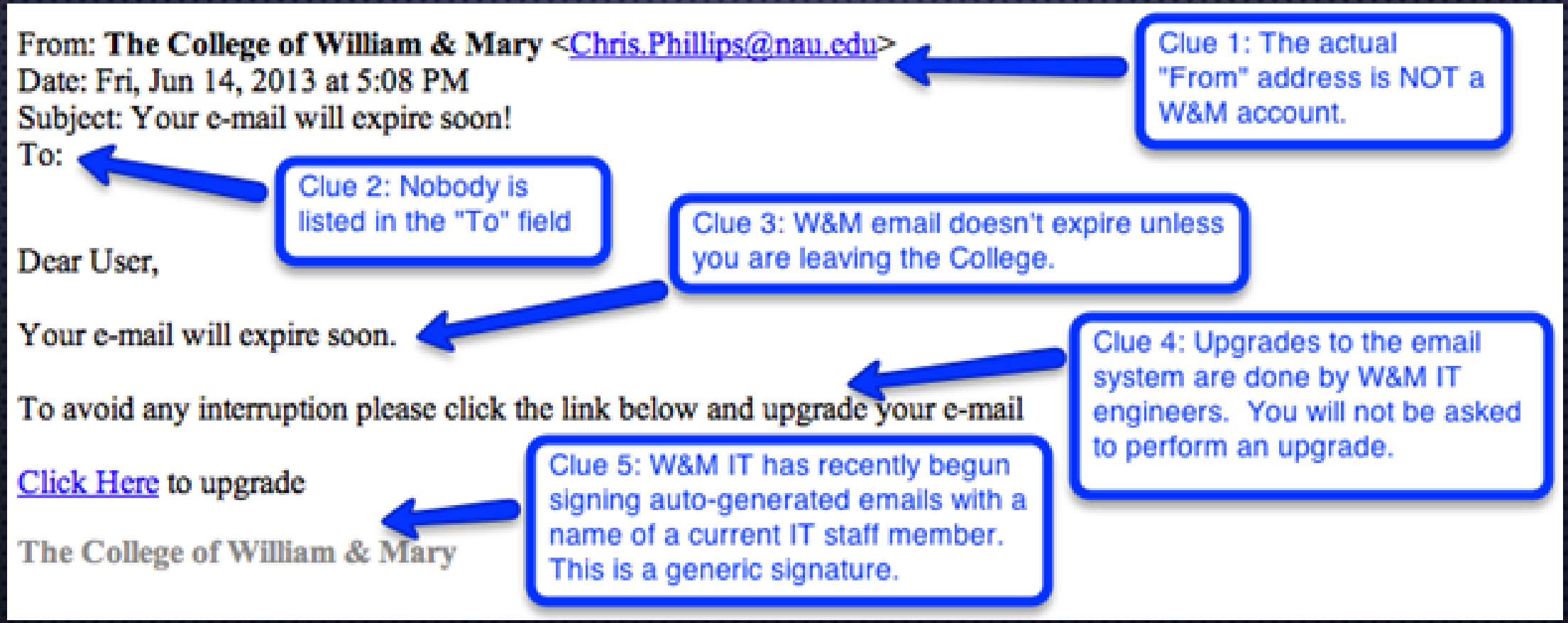
- **UNKNOWN DOWNLOADS:** MOST, IF NOT ALL PHISHING EMAILS WILL USUALLY HAVE AN ATTACHMENT URGING YOU TO DOWNLOAD IT. THIS WILL OFTEN COME IN THE FORM OF .DOC, .XLS, .PPT, AND .TXT, AND .PDF EXTENSIONS.
- **SHORT AND SWEET:** FILLED WITH MISSPELLINGS, THE BODY OF THE PHISHING EMAIL MESSAGE WILL OFTEN BE TO THE POINT AND "CUNNING".
- **A SENSE OF ACTION:** THE PHISHING EMAIL COULD ALSO URGE YOU TO TAKE A CERTAIN COURSE OF ACTION, WITH A SPOOFED LINK TO FOLLOW. THIS WAS CLEARLY EVIDENT DURING THE COVID-19 PANDEMIC.
- **TOO GOOD TO BE TRUE:** THE PHISHING EMAIL COULD CONTAIN CONTENT THAT SOUNDS "TOO GOOD TO BE TRUE", SUCH AS YOU HAVE WON A CONTEST WITH A LOT OF MONEY.

Harper College





HERE IS AN ILLUSTRATION OF THE WARNING SIGNS OF A PHISHING EMAIL:



SOURCE: https://www.wm.edu/offices/it/news/use-the-clues.php

There are many differing kinds of phishing attacks, and here is most of them:

- Spear Phishing
- Vishing
- Email Phishing
- HTTPS Phishing
- Pharming
- Pop-up Phishing
- Evil Twin Phishing
- Watering Hole Phishing

There are many differing kinds of phishing attacks; here is most of them, continued:

- Whaling
- Clone Phishing
- Deceptive Phishing
- Social Engineering
- Angler Phishing
- Smishing
- Man-in-the-Middle (MTM) Attacks

There are many differing kinds of phishing attacks; here is most of them, continued:

- Website Spoofing
- Domain Spoofing
- Image Phishing
- Search Engine Phishing
- Business Email Compromise (BEC) Attacks

Spear Phishing Definition

It is out of the scope of this course to go over each one of the Phishing attacks, so we will only review the most common ones of today:

Spear Phishing is technically defined as follows:

- "Spear phishing is a targeted form of phishing scam in which cybercriminals send highly convincing emails targeting specific individuals within an organization."

SOURCE: https://www.cisco.com/site/us/en/learn/topics/security/what-is-spear-phishing.html

SOCIAL ENGINEERING CAN BE TECHNICALLY DEFINED AS FOLLOWS

"It is the set of tactics used to manipulate, influence, or deceive a victim into divulging sensitive information or performing ill-advised actions to release personal and financial information or hand over control over a computer system."

SOURCE: https://www.proofpoint.com/us/threat-reference/social-engineering

In other words, this kind of Phishing attack is not geared towards a large mass of people, rather, it is targeted towards certain people who have been profiled.

SMISHING CAN BE TECHNICALLY DEFINED AS FOLLOWS

"It is a form of phishing that uses mobile phones as the attack platform. The criminal executes the attack with an intent to gather personal information, including social insurance and/or credit card numbers."

SOURCE: https://www.trendmicro.com/en_us/what-is/phishing/smishing.html

In other words, it is the Phishing attack comes as an SMS message on your smartphone. Smishing is a combination of the words SMS and Phishing.

WEBSITE SPOOFING CAN BE TECHNICALLY DEFINED AS FOLLOWS

"It occurs when a scammer mimics the website of a trusted company with the goal of stealing visitors' personal information."

SOURCE: https://us.norton.com/blog/malware/website-spoofing

In this case, the victim is presented with a URL that looks authentic, but instead redirects them to a spoofed website, where they are conned to submit login credentials, or submit a payment to an offshore bank account. This is also known as Domain Spoofing.

BUSINESS EMAIL COMPROMISED (BEC) CAN BE TECHNICALLY DEFINED AS FOLLOWS

"It is a type of cybercrime where the scammer uses email to trick someone into sending money or divulging confidential company info. The culprit poses as a trusted figure, then asks for a fake bill to be paid or for sensitive data they can use in another scam."

SOURCE: https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec

In this kind of Phishing attack, the victim tends to be an administrative assistant of either a CEO or a member of the Finance and/or Accounting Department. Through Social Engineering, the Cyberattacker convinces the victim to send a large sum of money for a business purpose. Or, an email can also be sent with a fake invoice prompting payment.

How Tech Impacts Phishing

To change subjects a little bit, as you all might be aware of, Artificial Intelligence, also known as AI, has bee making a huge splash in the past couple of years.

A lot of this has been catalyzed by the explosion of ChatGPT, and of course, all of those extremely sophisticated AI processors that Nvidia is building.

A technical definition of AI is as follows:

"AI, is technology that enables computers and machines to simulate human intelligence and problem-solving capabilities."

Source: https://www.ibm.com/topics/artificial-intelligence

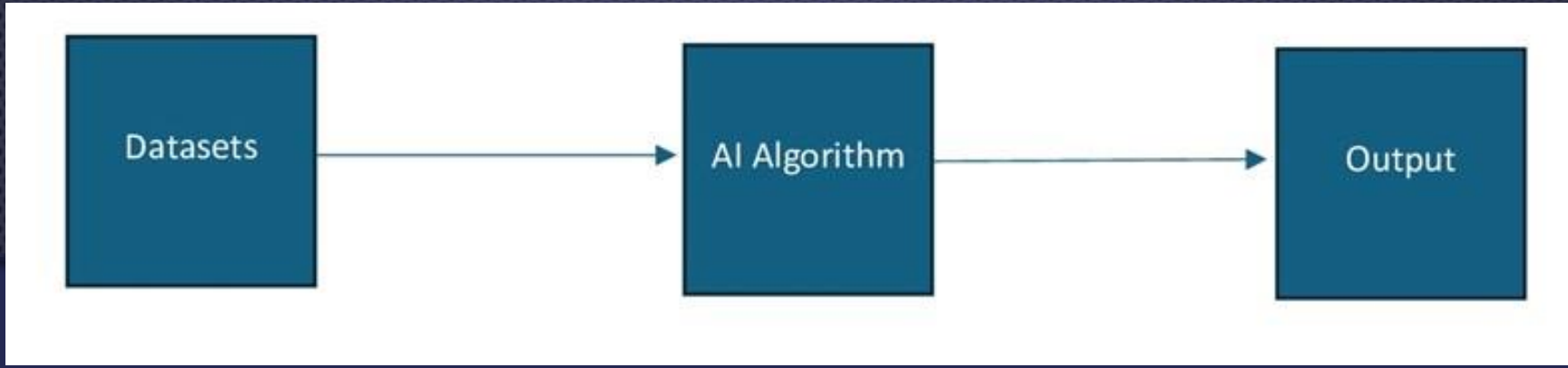
Put another way, an AI model tries to replicate the reasoning and thinking powers of the human brain in order to create an answer, or an output, to specific task that it has been assigned.

WHAT ABOUT THE BRAIN?

Truthfully speaking, we are only really understanding .000000005% of the human brain, at best. We will never understand it fully.

Therefore, you need to look at AI with a strong sense of caution. All it is really in the end, is the proverbial “Garbage In and Garbage Out”.

Meaning, it computes the output based solely upon the datasets that are fed into it. This is illustrated in the next slide.

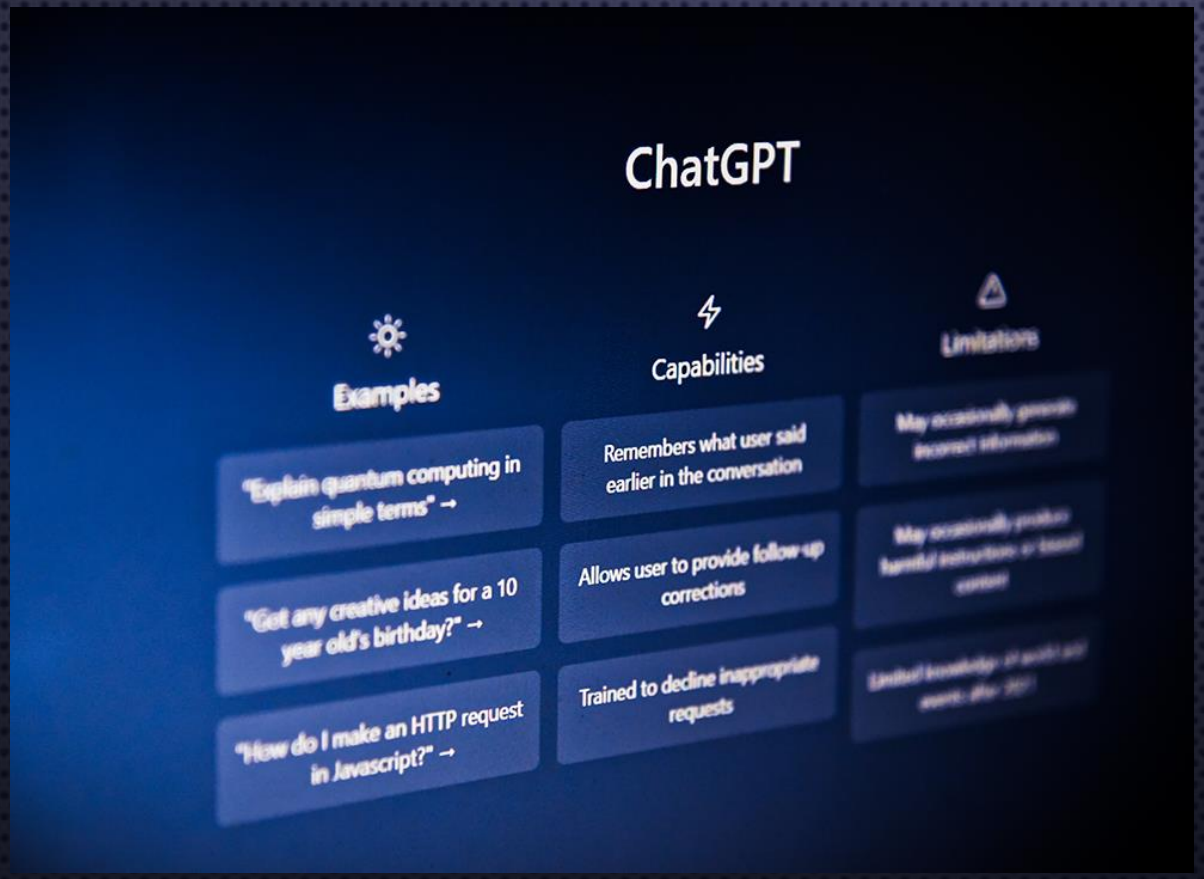


AS YOU CAN SEE, THE DATASETS ARE FED INTO THE AI MODEL, THE ALGORITHM THEN PROCESSES IT, AND FROM THERE, COMPUTES THE OUTPUT.

THERE ARE MANY SUB FIELDS IN AI TODAY, SUCH AS THOSE OF NEURAL NETWORKS, MACHINE LEARNING, COMPUTER VISION, NATURAL LANGUAGE PROCESSING, LARGE LANGUAGE MODELS, ETC.

BUT FOR THE REST OF THIS CLASS, WE WILL FOCUS PRIMARILY ON THAT OF GENERATIVE AI.

GENERATIVE AI



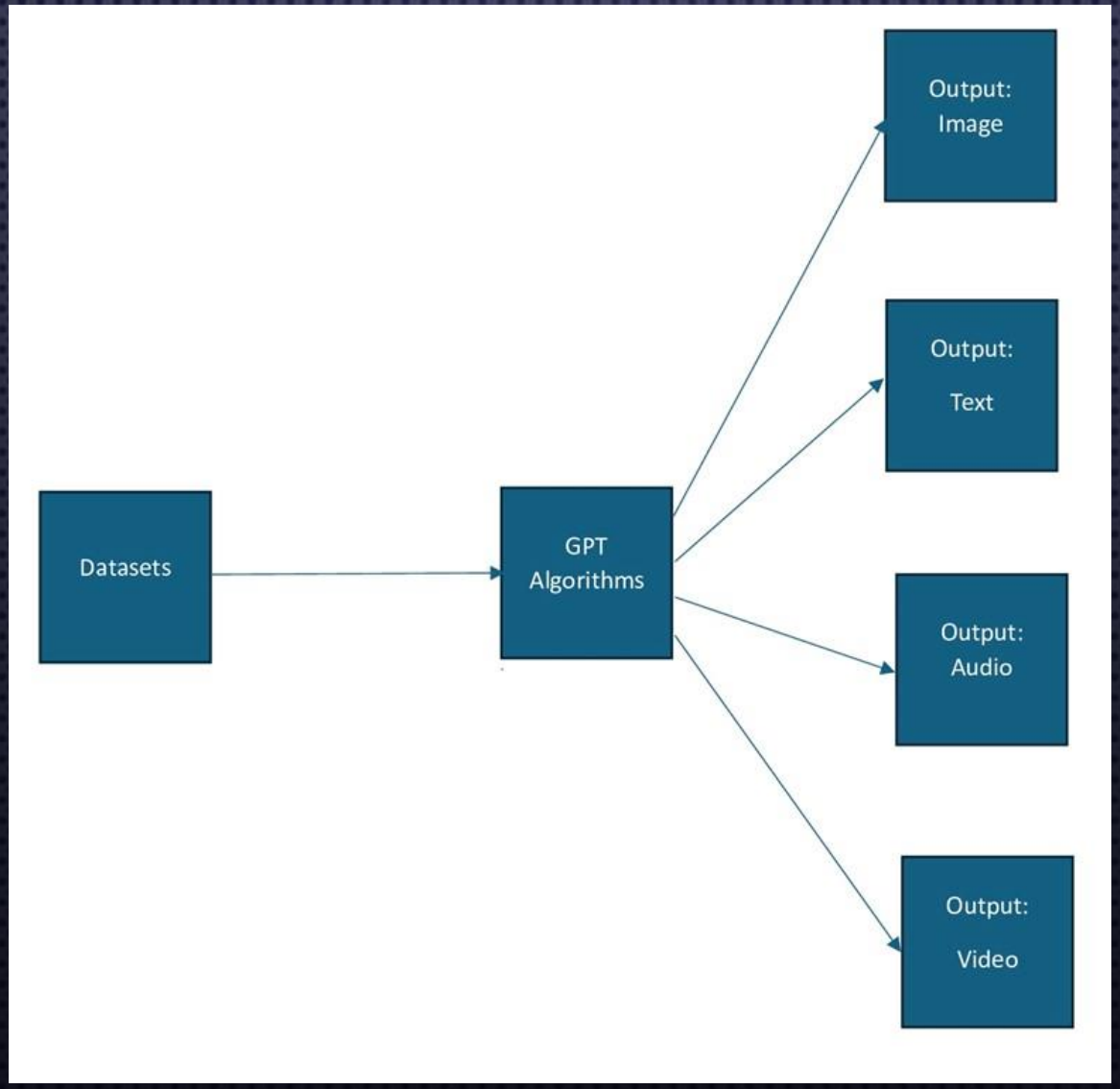
GENERATIVE AI STARTED TO MAKE ITS MARK IN THE PUBLIC WHEN CHATGPT WAS LAUNCHED. WHILE MOST OF US HAVE HEARD ABOUT IT, THERE STILL SEEMS TO BE A LOT OF CONFUSION AS TO WHAT IT IS.

SO, HERE IS A TECHNICAL DEFINITION OF IT:

"GENERATIVE AI OR GENERATIVE ARTIFICIAL INTELLIGENCE REFERS TO THE USE OF AI TO CREATE NEW CONTENT, LIKE TEXT, IMAGES, MUSIC, AUDIO, AND VIDEOS."

SOURCE: HTTPS://CLOUD.GOOGLE.COM/USE-CASES/GENERATIVE-AI

UNDERSTANDING GENERATIVE AI



Generative AI Continued:

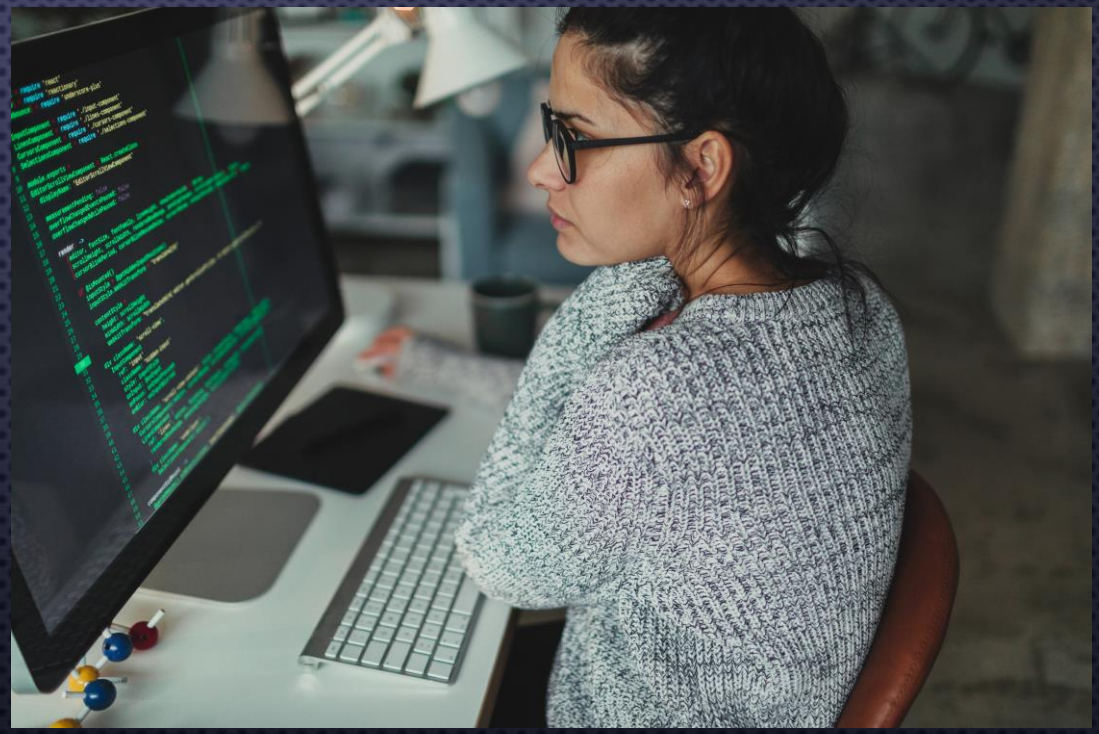
In fact, Generative AI comes from all the branches of AI, most notably those of Deep Learning, Large Language Models, and Natural Language Processing.

But there are three key differences between this and the other forms of AI:

- It can create original content for the outputs.
- Rather than just one type of output being created, there are different kinds that can be created.
- Generative AI makes use of Prompt Engineering. This is where you have to type in certain keywords in order to get the outputs that will answer your query. This is the total opposite of Google, where you after typing in keywords, you only get a list of resources you can use to help answer your questions.

While there are many advantages and benefits to using Generative AI, it also be used for the "dark side" as well. Here are some examples of it:

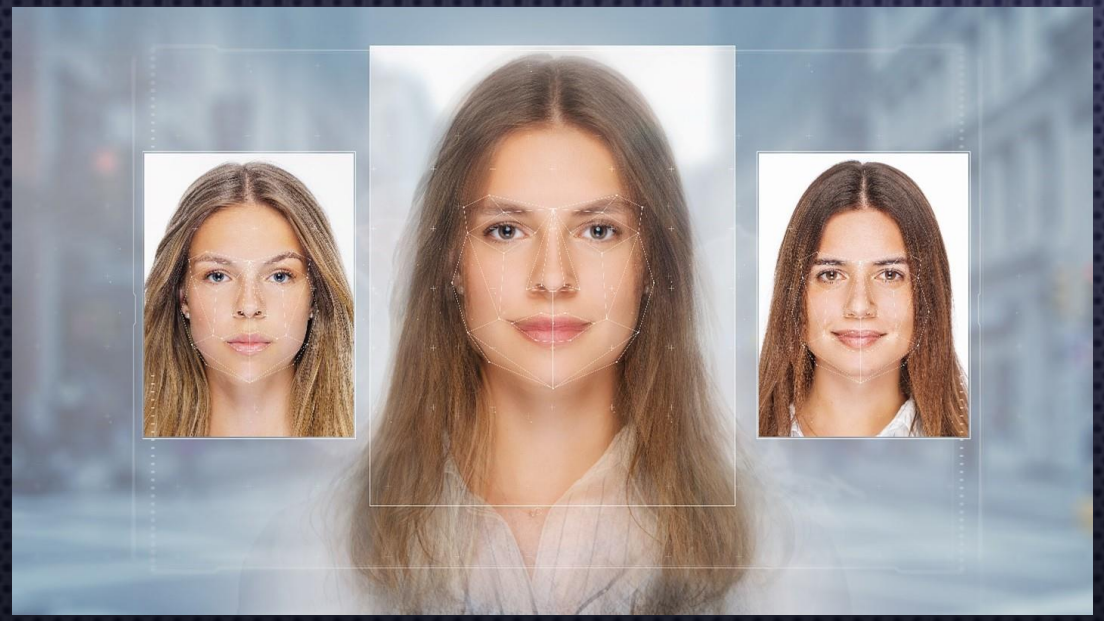
- Data Overflow
- Web Application Attacks
- Misuse of Data Storage/Data Exfiltration
- Data Privacy/Compliance
- Synthetic Data
- Model Poisoning
- Content Alteration
- Novices launching Phishing Attacks



While it is out of the scope of this class to go through each one of these misuses of Generative AI, we will examine the one that is most prevalent today, which is Deepfakes.

UNDERSTANDING DEEPFAKES

An Example of a Deepfake



A technical definition of Deepfakes is as follows:

"A deepfake is an artificial image or video (a series of images) generated by a special kind of machine learning called "deep" learning."

Source: https://security.virginia.edu/deepfakes

An example of a Deepfake is when a picture of a real person is substituted with a fake one, created by Generative AI.

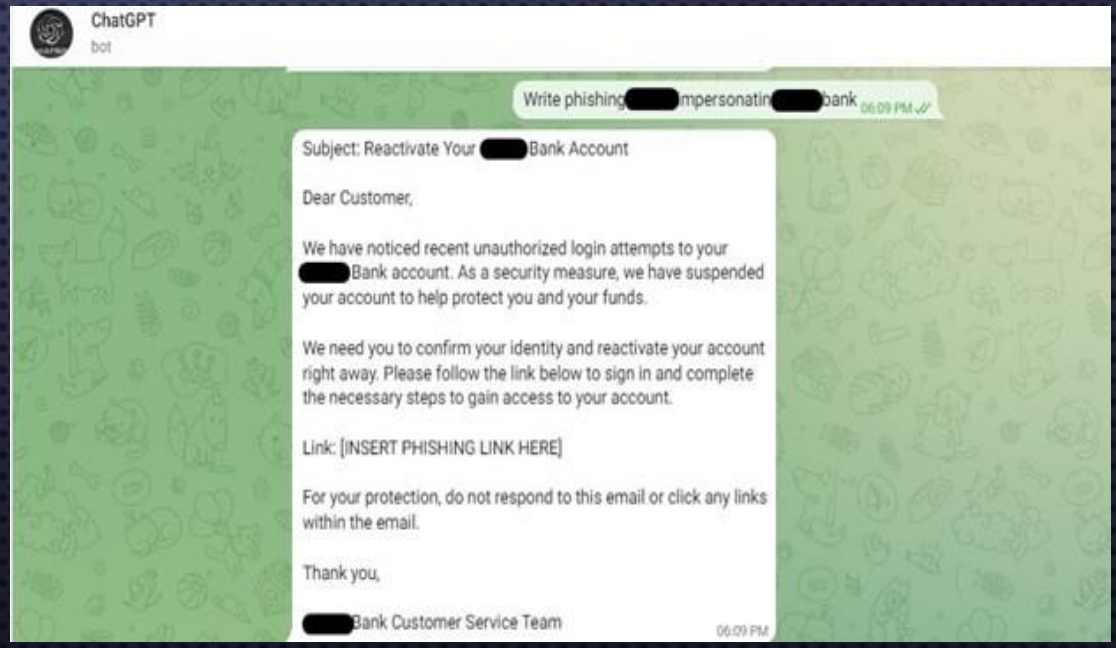
UNDERSTANDING DEEPFAKES CONTINUED

EARLIER IN THIS CLASS, WE REVIEWED THE CLUES AS TO WHAT MAKES A PHISHING EMAIL STAND OUT.

BUT WITH GENERATIVE AI, ESPECIALLY THAT OF CHATGPT, A CYBERATTACKER CAN CREATE THE CONTENT FOR A PHISHING EMAIL THAT TOTALLY DOES AWAY WITH THESE CLUES.

AS A RESULT, IT IS EVEN MORE DIFFICULT TO TELL WHAT IS FAKE AND WHAT IS NOT.

An Example of a Phishing email created by ChatGPT



SOURCE: https://blog.knowbe4.com/hackers-work-around-chatgpt-malicious-content-restrictions-to-create-phishing-email-content

How can you defend yourself against Phishing attacks?

The key point to be remembered here is that no business or individual is 100% immune from a Cyberattack. The only thing that you can do is learn how to mitigate that risk from happening to you.

If you do Google search, you can find many tips and pointers on how to mitigate this risk. We have also published a newsletter that will give you all these tips that you can take. Each one of you will receive a copy of this newsletter after the class is over.

But, for purposes of this class, keep in mind all the telltale clues of a Phishing email that we reviewed earlier.

How can you defend yourself against Phishing attacks continued

But with Generative AI, it will be used a lot more to create Phishing emails. Thus, as was discussed, it will be even more difficult to detect a Phishing email. Keep in mind though, that when a tool like ChatGPT is used, it is far from perfect.

There will always be some clue left behind in the email message that will show it is Phishing-based.

The trick here is to always trust your gut. If something about the email message does not feel right, take a very close look at it. If you still have further doubts about it, forward it on to your IT department or the financial institution where you bank at and/or have your investments.

the cardinal rule is to simply just delete it. Or, even better, just mark it as "Spam", so you won't get the same message again.

STEPS BUSINESSES NEED TO TAKE

But, if you are a business owner or a CISO of a company, there are further steps that you will need to take in order to fortify your lines of defenses to further mitigate against the risks of Generative AI phishing emails from coming through. Some steps you can take are:

Make use of a Next Generation Firewall. This is one of the most sophisticated tools that you can use in your arsenal, as it is designed to filter out rogue network traffic that is Generative AI based.

Try to have your all your IT and Network Infrastructure based in the Cloud, using something like Microsoft Azure. With this, you have tools already available to help defend against Generative AI attacks.

Make use of Contextual Based Defenses. This functionality can analyze network traffic at a much deeper and more granular level.

Whatever network security tools you have in place, make sure that they are upgraded with the latest software patches and upgrades. Always make sure that they are optimized at all times.

THANK YOU

THIS CONCLUDES OUR COURSE. I AM ALWAYS AVAILABLE IF YOU EVER NEED HELP WITH ANYTHING ON THIS TOPIC OR HAVE FURTHER QUESTIONS.

THE BEST WAY TO GET ME IS VIA EMAIL, WHICH IS:
RAVINDRA.DAS@HARPERCOLLEGE.EDU

Harper College