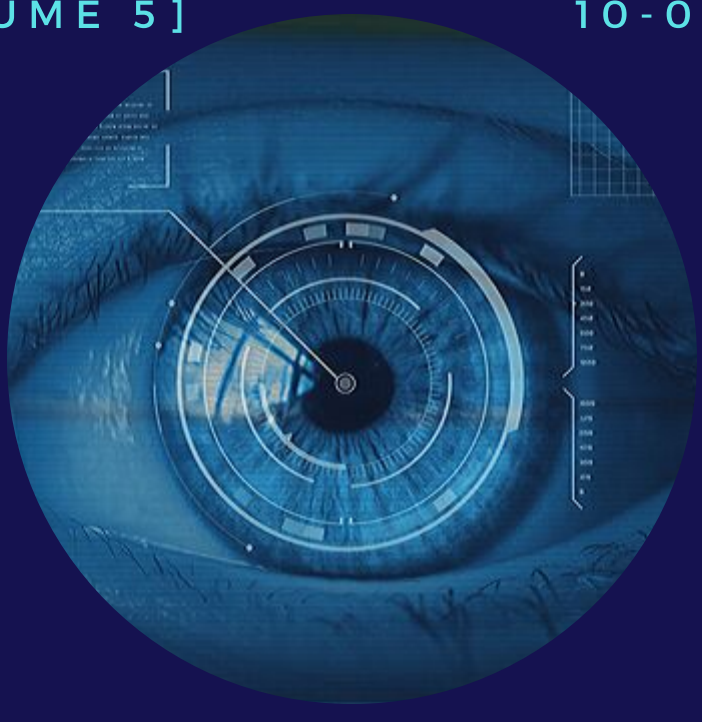
WELCOME TO THE GEMINI IBD INFOGRAPHICS NEWSLETTER

[VOLUME 5] 10-01-2019



WHAT IS PHISHING & HOW TO AVOID IT

INTRODUCTION TO PHISHING

What is Phishing? It can be defined as follows: "It is an attempt, originally via a message or email, to lure computer users to reveal sensitive personal information such as passwords, birth dates, credit cards, and social security numbers." (SOURCE: 1).

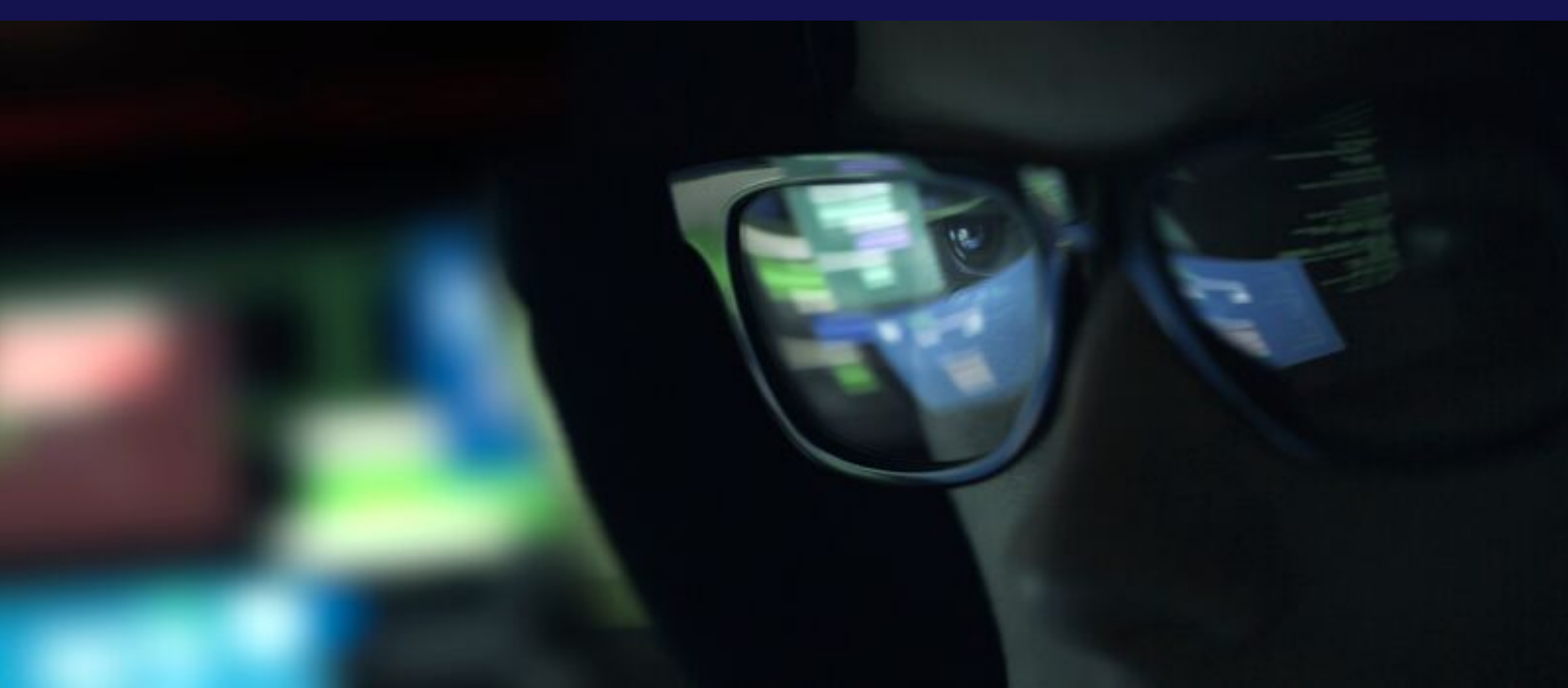
Phishing is a form of Cyberattack that goes back a long time, and in fact, is one of the oldest forms of threat vectors that still exist out there. But, there are many variants coming out, which is making it more difficult to notice and more covert. There are:

~156 million phishing emails are sent worldwide;

~This results in 80,000 clicks — PER DAY;

~All of this costs Corporate America almost $4 Million on an annual basis. (SOURCE: 1)

THE OVERALL SIGNS OF A PHISHING ATTACK



In order to launch this kind of attack, the message to the recipient pretends to be from an official representative of a website or another institution that the intended victim has more than likely done business with (e.g., PayPal, Amazon, UPS, Bank of America, etc.).

Phishing attacks can occur in different forms. For instance, it could be a scam phone call (such as the person claiming to be from the IRS, and states that there is a warrant for your arrest because you owe back taxes), a snail mail (this could be a postcard or even a letter claiming to be from a collector claiming that you thousands of dollars in unpaid bills, and to call the number provided), and by Email.

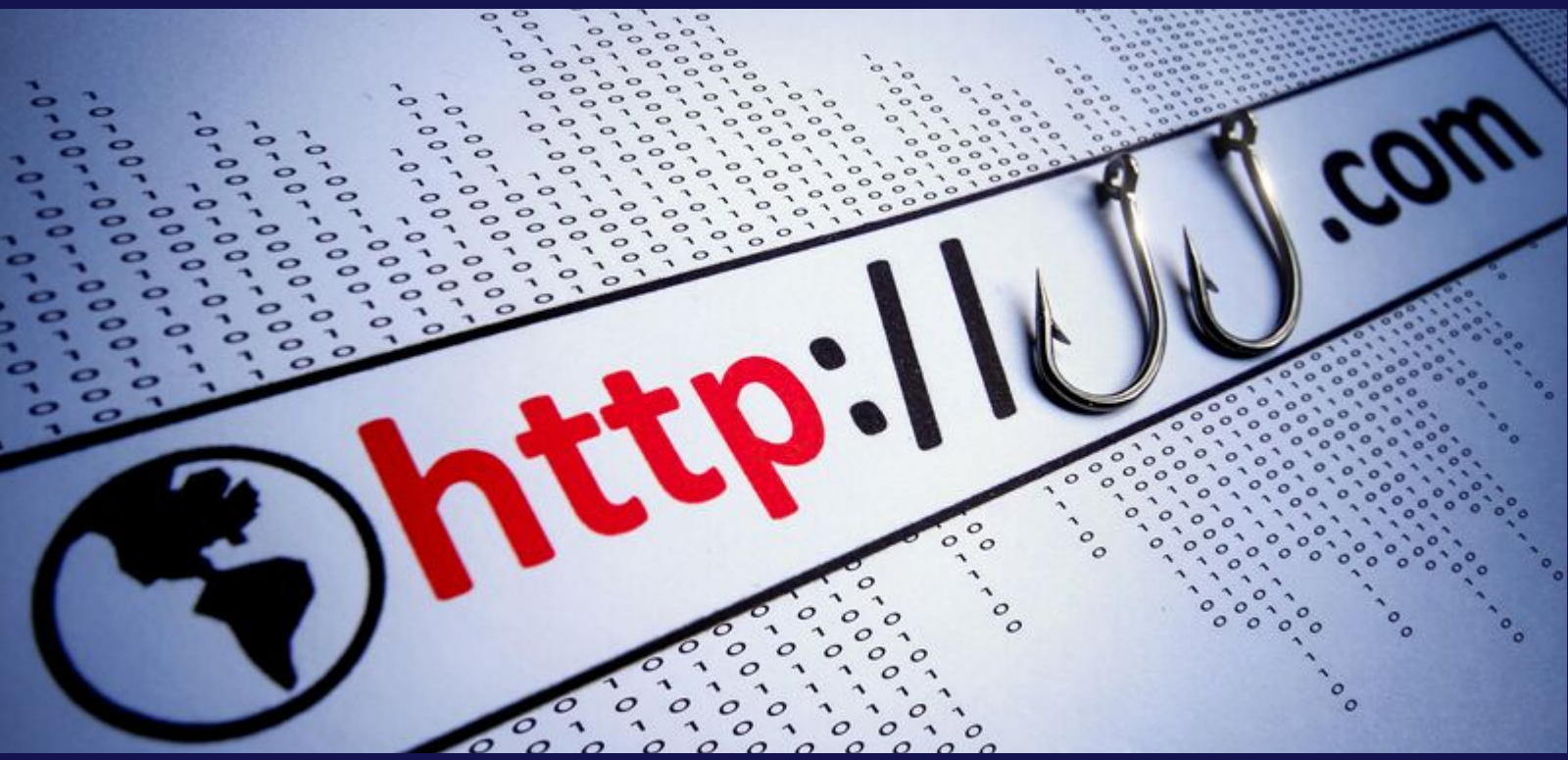
Right now, the primary method of Phishing has always been and continues to be by Email. These are some of the general, telltale signs of a Phishing based Email...

- The subject line of the Email will contain a sentence of interest, that will entice the victim into actually opening the Email message. For example, this could be stating “iPad giveaway,” “fraud alert”, or other type of intriguing subject line.
- The email itself may contain the company’s logo and phone number, in order to give it a sense of legitimacy.
- It looks like a personal email from a friend or relative who wants to share something with you.
- There is very often a malicious link in the body of the Email message. Once the intended victim clicks on the provided link, instead of being directed to the real and authentic website, they are taken to a fake, where they unwittingly enter all their information as prompted.
- Once this done, the Personal Identifiable Information (PII) is then captured by the thieves and used immediately, sold on the black market for nefarious purposes (such as the Dark Web), or even both.
- Also, many times the user’s computer is also infected, sending out phishing emails from their address books and continuing the rampage.

THE ORIGINATIONS OF PHISHING

Phishing goes all the way back to 1990.
Here is a chronological history of it:

1. The concept of phishing can be traced back to the early 1990s via America Online, or AOL. A group of hackers and pirates came together and called themselves the warez community are considered the first true “phishers.” In an early scam, they created an algorithm that allowed them to generate random credit card numbers. When a match real card was matched, they were able to create an account and spam others in the AOL community.
2. By 1995, AOL was able to stop the random credit card generators, but the warez group moved on to other methods, pretending to be AOL employees and messaging people via AOL Messenger for their information in Social Engineering Attacks.
3. On January 2, 1996, the word “phishing” was first posted in a Usenet group dedicated to American Online.
4. By the mid 1990’s phishers switched to email communications, which were easy to create, cheap to send out, and made it nearly impossible for them to get caught.
5. In September 2003, phishers began registering domains that were similar to popular companies such as Yahoo (yahoo-billing.com) and Ebay (ebay-fulfillment.com).
6. In October, 2003, Paypal users were impacted by the Mimail virus. When they clicked on a link contained in a phishing email, a popup window appeared claiming to be coming from Paypal. It instructed them to enter their user/password, which was immediately sent to the Cyberattackers.
7. In 2004, voters for presidential candidate John Kerry received an official-looking email, asking them to donate via an authentic looking (but malicious link). It turned out to be a scam operating in both India and Texas that had no connection to the Kerry campaign.



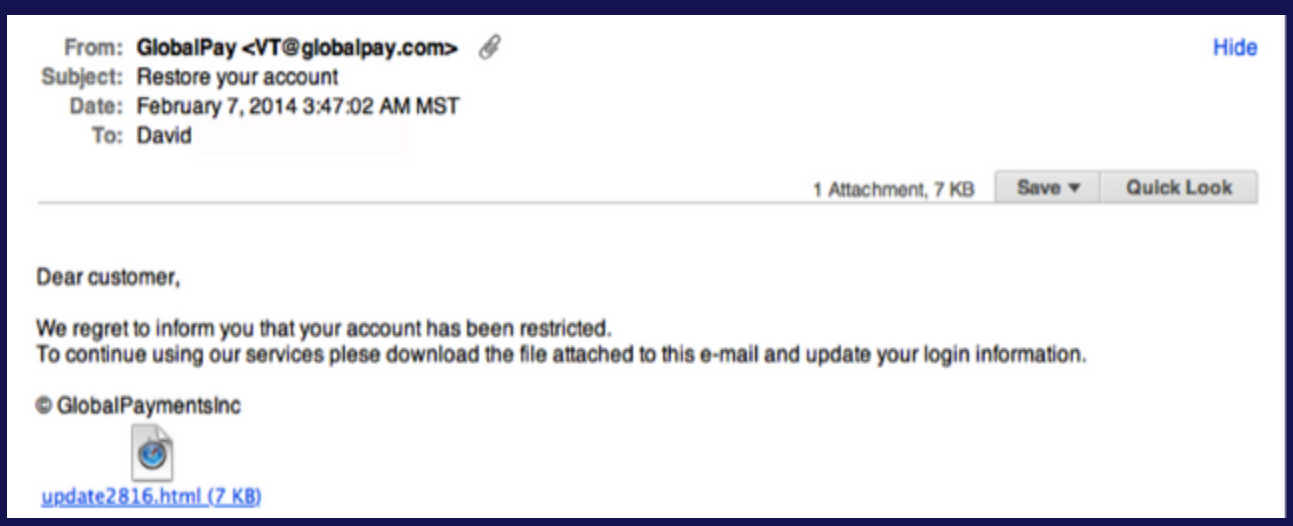
MORE SPECIFIC SIGNS OF A PHISHING EMAIL

Although we have presented the general signs of a Phishing Email, here are the more specific clues that you may become a victim.

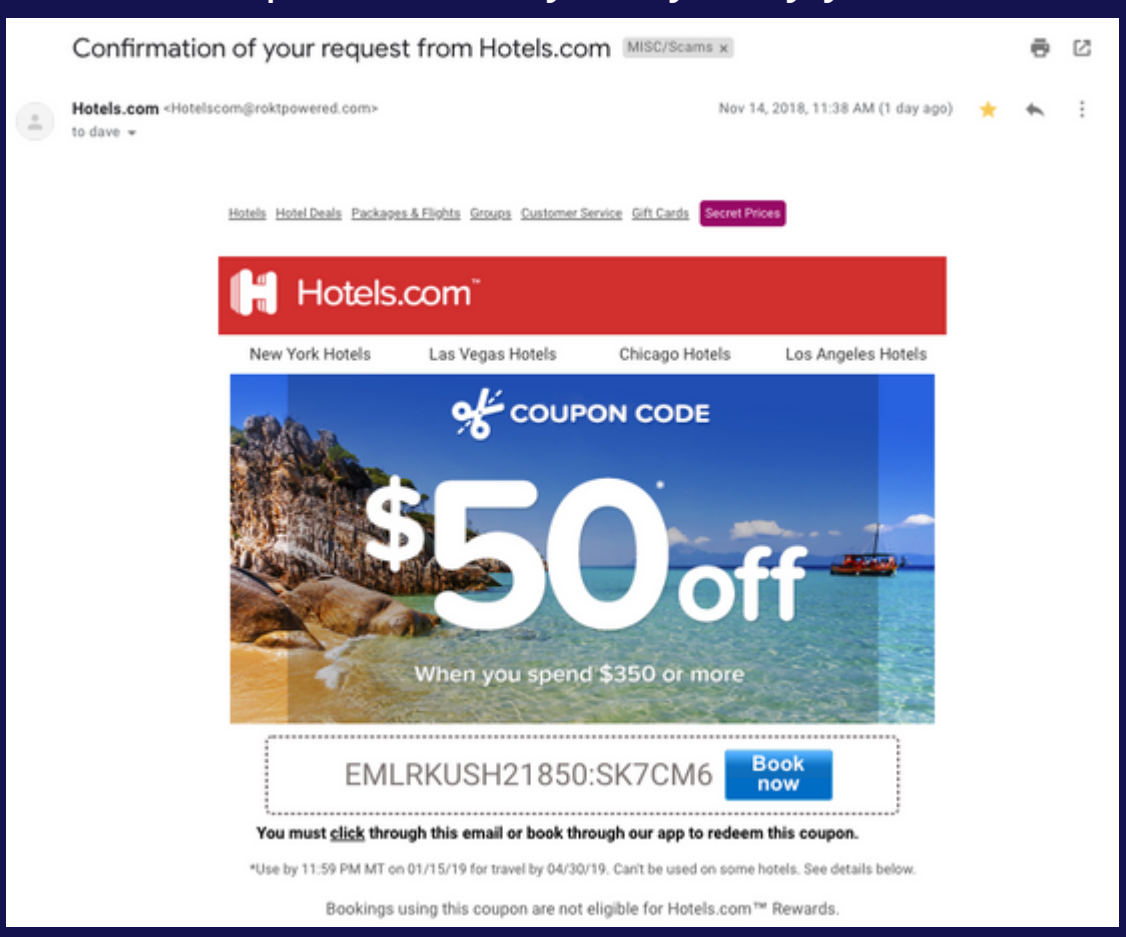
- There is an unfamiliar tone or greeting to the Email message;
- It consists of many grammar and spelling errors;
- There are numerous inconsistencies in the Email address (primarily the sender), links and domain names in the Email message itself;
- There is a strong threats or a sense of urgency to the Email message;
- There are suspicious attachments included (primarily those of .XLS and .DOC file extensions);
- They ask for unusual requests that are out of the norm;
- The Email message is short and sweet in order to play tricks on your memory;
- The recipient did not initiate the conversation; very often this is a hook is to inform the recipient he or she has won a prize, will qualify for a prize if they reply to the email, or will benefit from a discount by clicking on a link or opening an attachment;
- There is often a request for credentials (such as your username/password), payment information (like your credit card number), or other personal details.

EXAMPLES OF PHISHING BASED EMAILS

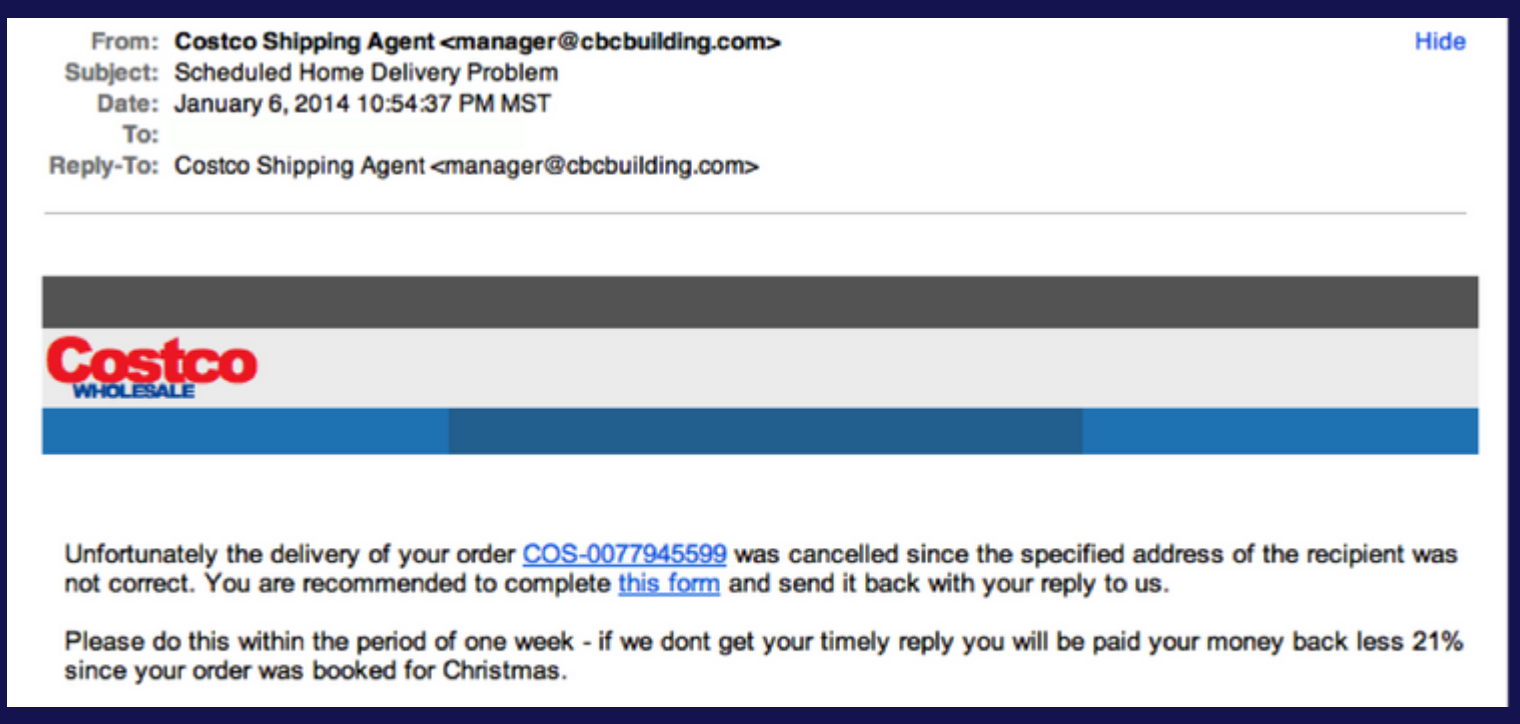
Legitimate companies don't request your Personal Identifiable information (PII) via email.



Real companies usually call you by your name.



Authentic companies have real domain Emails.



A real business will know how to spell.

From: **Best Buy <BestBuyInfo@fashionlab.com.ua>** Hide
Subject: Special Order Delivery Problem
Date: December 20, 2013 11:06:08 AM MST
To: dave
Reply-To: Best Buy <BestBuyInfo@fashionlab.com.ua>

My Besy Buy ID: 002024460
Reward certificate(s) available.

BEST BUY

WEEKLY DEALS GIFTS

Tvs Computers & Tablets Cell Phones Appliances Cameras Video Games Audio

Sir/Madam,

Your order BBY-4983814314 has not been delivered because the specified address was not correct.
Please fill this form and send it back with your reply to this message.

If we do not receive your reply within a week we will pay your money back less 17 because your order was reserved for the time of Christmas holidays.

Best Buy 7601 Penn Avenue South, Richfield, MN 49584-7655

BEST BUY, the BEST BUY logo, the tag design, BESTBUY.COM, GEEK SQUAD, the GEEK SQUAD logo, MY BEST BUY, REWARD ZONE, BEST BUY MOBILE and the BEST BUY MOBILE logo are trademarks of BBY Solutions, Inc. All other trademarks or trade names are properties of their respective owners.

A real business will not force you to their website.

From: **Manager Daniel Bridges <daniel_bridges33@gulfslipformpaving.com>**
Subject: Information
Date: August 26, 2013 1:25:12 AM MDT
To: dave
Reply-To: Manager Daniel Bridges <daniel_bridges33@gulfslipformpaving.com>

USPS.COM

Notification

Our courier couldnt make the delivery of parcel to you at 20th August.
Print label and show it in the nearest post office.

Print a Shipping Label NOW

Legitimate companies don't send unsolicited attachments.

From: "Bank"<payment@epayment.com>
Subject: Re: new payment on your account
Date: March 24, 2014 10:39:01 AM MDT
Reply-To: <bankwiretransferdepartment@gmail.com>

Please find attached bank slip for new payment on your account.

Regards,

Account Department.

ZIP

new payment.zip

A real company has links in their Emails with legitimate URLs.

From: **Nokia <info@news.nokia.com>** Hide
Subject: SAVE YOUR STUFF! Sign in to your Nokia account before it disappears forever!
Date: February 7, 2014 2:38:02 AM MST
To:
Reply-To: Nokia <info@news.nokia.com>

NOKIA

SAVE YOUR STUFF!

We noticed you haven't used your Nokia account to access Nokia services in quite a while. To protect your privacy, this account will be deleted in 14 days, so sign in now.

If you haven't experienced Nokia services recently, they're worth another look. And you may want to keep any maps, locations, email, music, reviews, or other stuff that is associated with your account.

It just takes a few seconds to sign in to your Nokia account.

We hope to see you soon.

Sincerely,
The Nokia account team

THE COSTS OF A PHISHING ATTACK

Phishing Attacks can take an enormous toll on anybody, any country, and any economy. Here are some of the numbers.

- The average cost to a business in one year is a staggering $3.86 Million;
- Business Email Compromise (aka BEC, a variant of Phishing) has cost companies around the world $12.5 Billion;
- The largest Phishing Attack was on a healthcare organization; the Spear Phishing Emails (yet another variant) cost $16 Million;
- Phishing Attacks target heavily the financial sector – it costs one financial firm $18 Million in one single year just to recover from Phishing Attacks;
- It costs $135/hour for a business to recover from a Phishing Attack;
- If you are sued because your company was hit by a Phishing Attack, it will cost you $260/hour in just legal fees;
- Identity Theft Protection services can cost as much as $9.99 per employee per month;
- If you have a call center, and they have to field calls answering questions about a Phishing Attack, it will cost your company $14.53/hour;
- Phishing victims have to be notified at least once by snail mail that they have potentially become a Phishing victim. This costs on average, $1 per letter. That may not sound like a lot, but what if you have to send out thousands or even a million of these letters?
- Phishing Attacks have risen by 65% from 2015 to 2016:

793,340 Phishing Emails were sent out in 2015

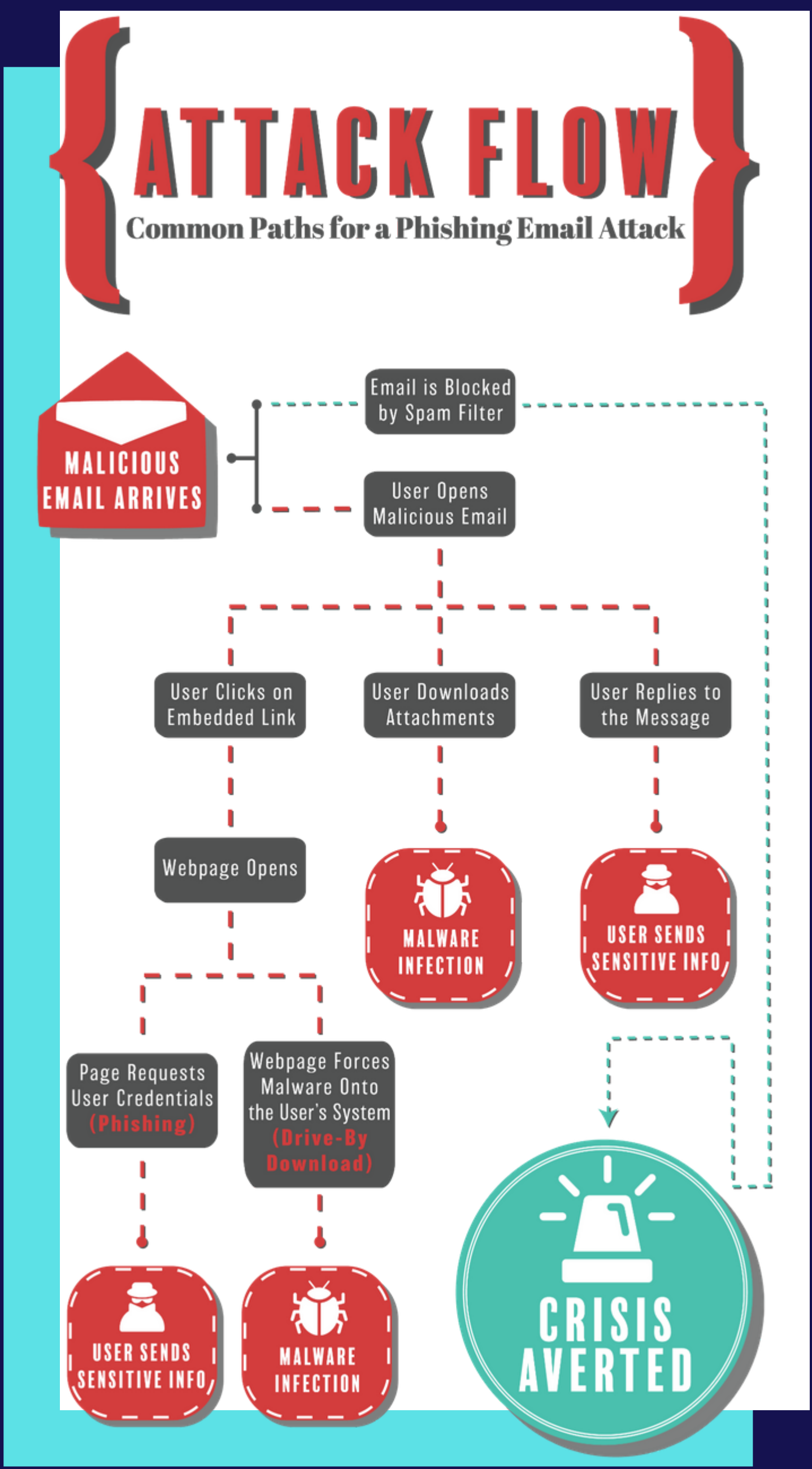
1,220,523 Phishing Emails were sent out in 2016

- 91% of Cyberattacks first start with a Phishing Email;
- 30% of all Phishing Emails get opened;
- 9 out of 10 Phishing Emails have carried a Malware payload with them;
- 12% of users click on the malicious link that is contained in the Email message;
- 1.5 Million new spoofed websites are created each month;
- 95% of all attacks on Network Infrastructures are done by Spear Phishing;

- In 2018 alone, 76% of all businesses in Corporate America reported being a victim of a large scale Phishing Attack;
- Fake Invoices are the #1 bait that is used to lure in the victim in a Phishing Attack;
- Apple Store ID's and passwords are the #1 stolen credential in Phishing Attacks.

THE ANATOMY OF A PHISHING EMAIL ATTACK

Here is how a Phishing Email Attack is launched, and gets delivered to the intended victim.



1. The Email is either blocked by a spam filter or it gets delivered. Blocking the Phishing Email before it even reaches its intended recipient is the only way to stop an attack before it starts. But if the Phishing Email bypasses the Spam Filter, it will likely be delivered to the victim.

2. The victim then either clicks a link, downloads an attachment, or replies to the Phishing Email

The Embedded Link:

The first route is for the victim to click a malicious link in the Phishing Email that loads up a spoofed website. From here, the webpage will likely open one of the following: A form requesting the victim's credentials, granting the attacker access to their PII; Redirect the victim to a webpage that forces Malware to download onto their computer. This attack is known as a drive-by download.

The Malicious Attachment:

Cyberattackers can also coax the victim into downloading a malicious attachment. The result can be a nasty malware infection served with a major data loss. Some of the most common types of malicious attachments appear as .DOC, .ZIP, or .XLS file extensions.

The Direct Reply:

Cyberattackers have gotten sensitive information by simply posing as a trusted contact of the victim. Fooled, the victim responds with sensitive information by replying to the Email, or even calling the phone number that is provided in the Email message.

THE TYPES OF PHISHING ATTACKS

There are numerous types of Phishing Attacks, such as the following.

Email Spoofing, which can be done in one of three ways:

- Sending an Email through a familiar Email ID,
- Sending an Email impersonating the C-Suite;
- Impersonating the identity of a business or corporation and asking employees to share internal data (Social Engineering)

From: **avlor.hr@gmail.com**

To: bruce@avlorcloud.info

Subject: Message from human resources

Dear Bruce,

An information document has been sent to you by the Human Resources Department. **Click here to Login** to view the document.

Thank you

HR Department

Avlorcloud University of California

Mass Target Phishing Emails are sent to potential victims such as receipts, payment reminders, or gift cards.

Subject: Citibank Email Verification

Dear Citibank Member,

This email was sent by the Citibank server to **verify your email address**. You must complete this process **by clicking on the link below** and entering in the small window your **Citibank number and PIN that you use on ATM**. This done for your protection – because some of our members no longer have access to their email addresses and we must verify it.

To verify your email address and access your bank account, Click on the link below:

http://www.citibank.com/domain/redirecthubjZhgefyuXCgkygfDBHUIvhdfrktghDgkjhdlhgu58638tghkjt

URL Phishing is where Cyberattackers use a malicious link to infect the target. Watch for both hidden links...

Subject: Account alert

Important message from Wells Fargo

Wells Fargo is consistently seeking to improve the service that is offers to its old and new customers. Every time you log on to our online service to check to ensure that your current status and account settings will give the required level of performance and security.

As the result we need you to visit our online service portal by following the reference given below and provide your urgent phone number where we can reach anytime during the day.

<Click Here>

Thanks for your patience as work together to protect your account

Sincerely

Wells Fargo Bank, N.A

Important: Please update your records on or before 24 hours

...and misspelled links...

Subject: Citibank Email Verification

Dear Citibank Member,

This email was sent by the Citibank server to verify your email address. You must complete this process by clicking on the link below and entering in the small window your Citibank number and PIN that you use on ATM. This done for your protection – because some of our members no longer have access to their email addresses and we must verify it.

To verify your email address and access your bank account, **Click** on the link below:

http://www.citiibank.com/domain/redirecthubjZhgefvuXCgkvgf

The subdomain attacks are aimed specifically towards the non-technical employees of a business or corporation.

Mon 30/01/2017 12:21

LinkedIn Email Confirmation <emailconfirm@linkedin.example.com>

Please confirm your email address

To REDACTED

LinkedIn

Fake link

Click here to confirm your email address.

http://reformadecomunidades.com/rummers.php
Click to follow link

If the above link does not work, you can paste the following address into your browser:

https://www.linkedin.com/e/eGx1ClQBEZhdl1jlu67Nsrsyn0QNrdgavOxiBJIMO

You will be asked to log into your account to confirm this email address. Be sure to log in with your current primary email address.

We ask you to confirm your email address before sending invitations or requesting contacts at LinkedIn. You can have several email addresses, but one will need to be confirmed at all times to use the system.

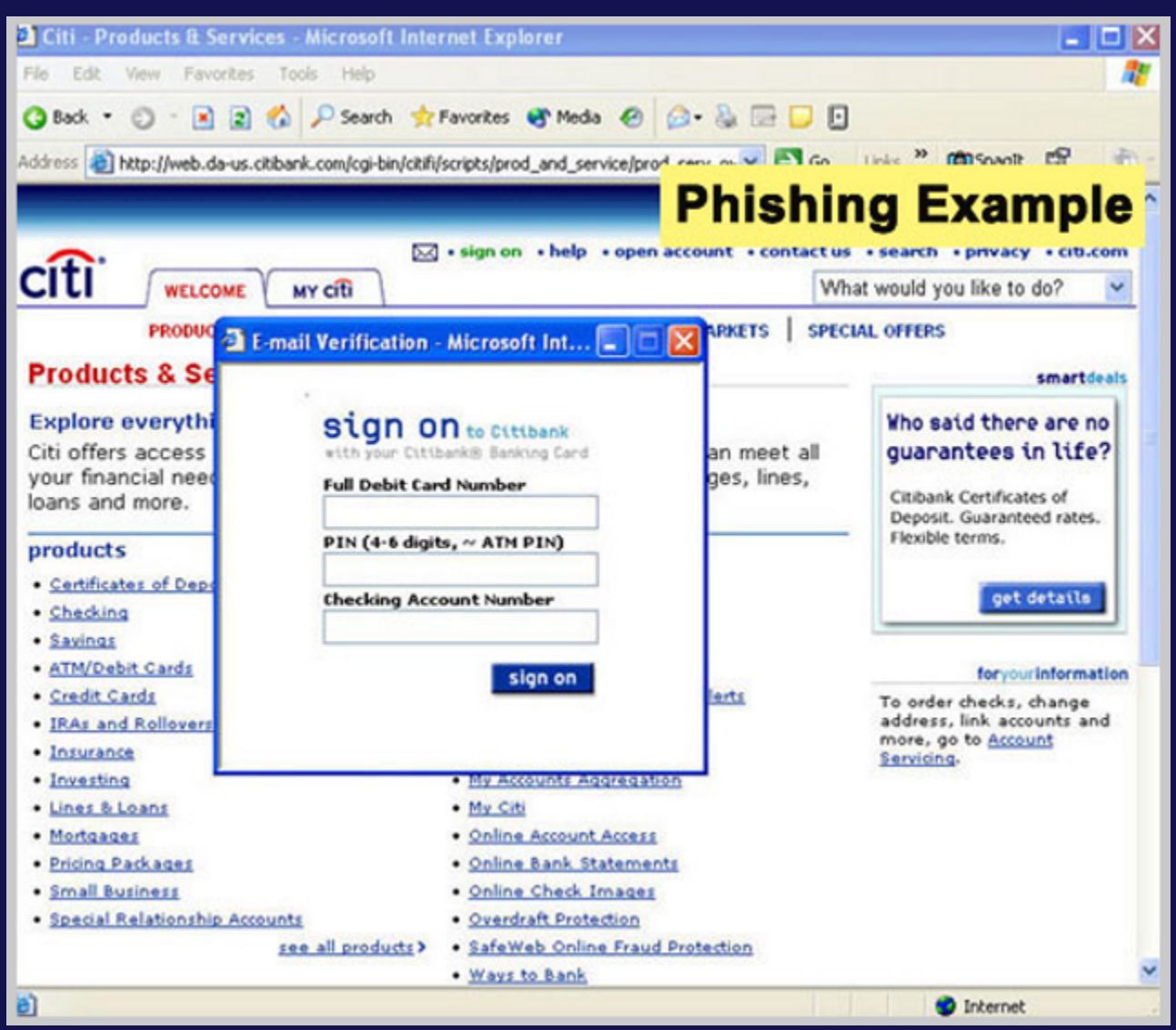
If you have more than one email address, you can choose one to be your **primary email address**. This is the address you will log in with, and the address to which we will deliver all email messages regarding invitations and requests, and other system mail.

Thank you for using LinkedIn!

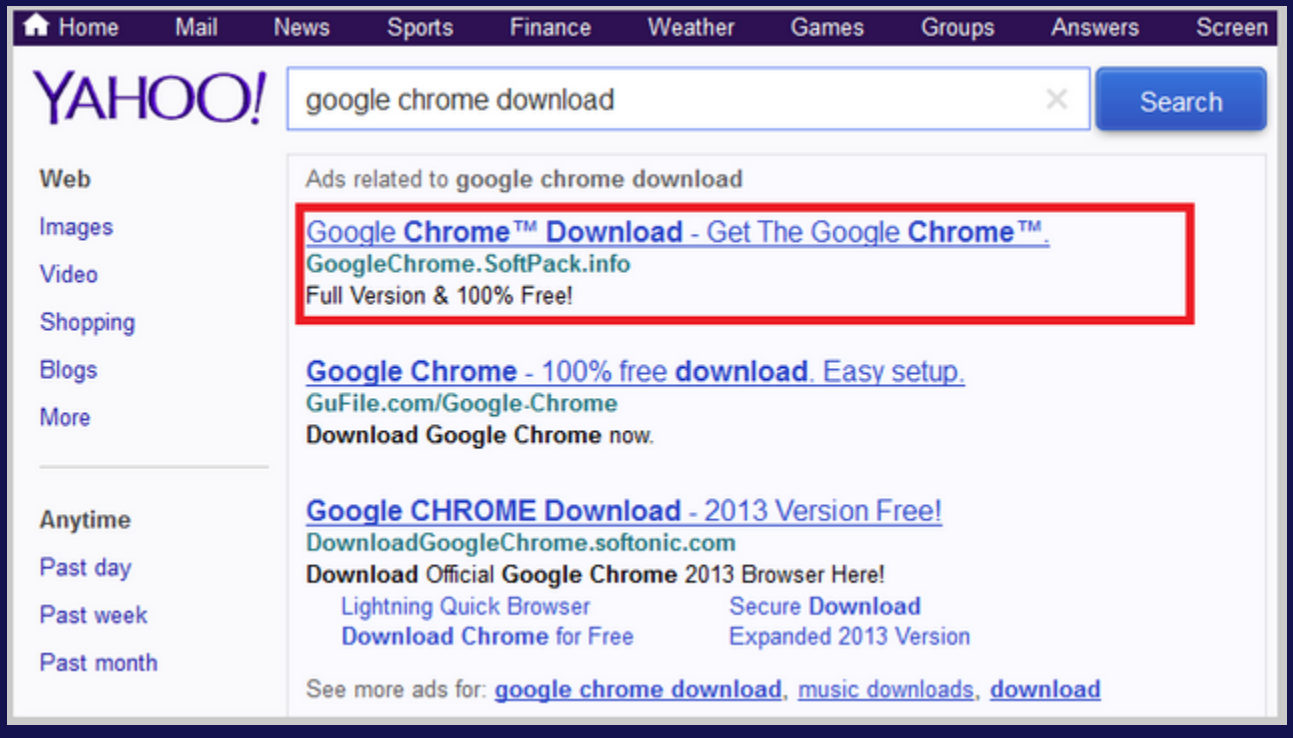
--The LinkedIn Team
http://www.linkedin.com/

© 2017, LinkedIn Corporation

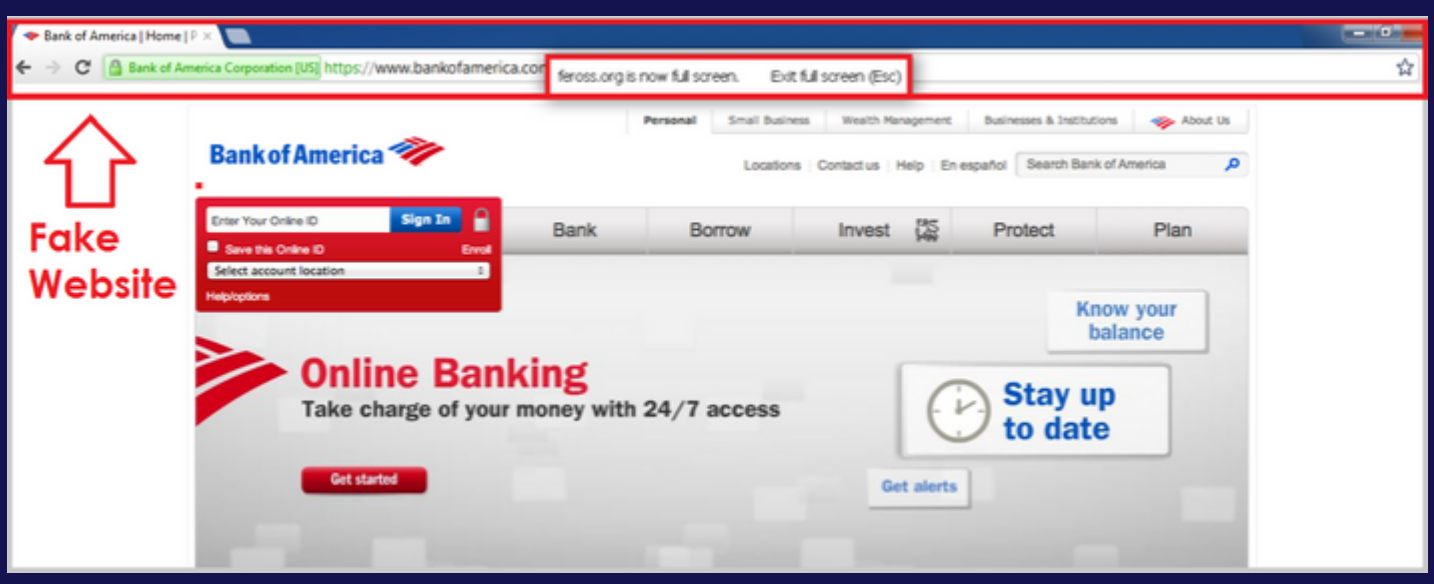
Pop up messages are the annoying pop up windows that appear in your web browser.



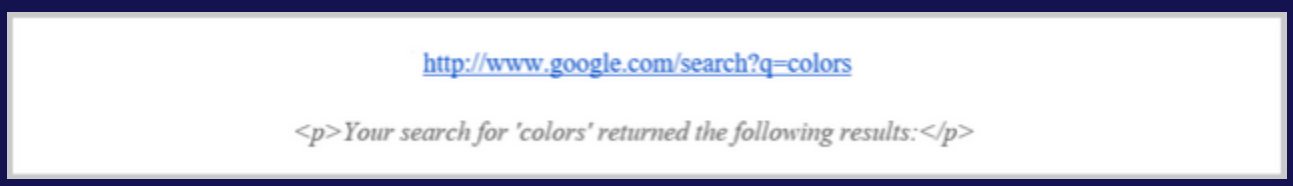
The search engine attack is when the Cyberattacker executes a paid campaign that is optimized for certain keywords.



Website spoofing is when a Cyberattacker creates and publishes a website by copying the design, content, and user interface of a legitimate and authentic website.



Scripting or Cross-Site Scripting (XSS) uses malicious source code scripts that are deployed onto the victim's computer or wireless device using Emails as the source.



You may also experience one of the following:

- The Man-in-the-Middle Attack is where the Cyberattacker impersonates themselves on both sides in order to access confidential information such as financial transactions, and other forms of PII.

  There are two types of Spoofing Techniques used:
  1-ARP spoofing:
  This is an attack in which the Cyberattacker sends a fake ARP (Address Resolution Protocol) message over a Local Area Network (LAN). This links the attacker's MAC (Machine Address) address to the IP address of a legitimate computer or server on the network.

  2-DNS spoofing:
  Domain Name System (DNS) spoofing or DNS Cache Poisoning is a form of Cyberattacking that corrupts the DNS data in the resolver cache, causing the DNS server to return incorrect result records.

- In a Clone Phishing Attack, a previously-sent email that contains any link or attachment is used as a true copy to create an almost identical or cloned Email. The Cyberattacker then replaces the link or attachment in the email with a malicious link or attachment.

- Image phishing or what is also known as a "Phishing Image". It can happen in one of two ways (or even both):

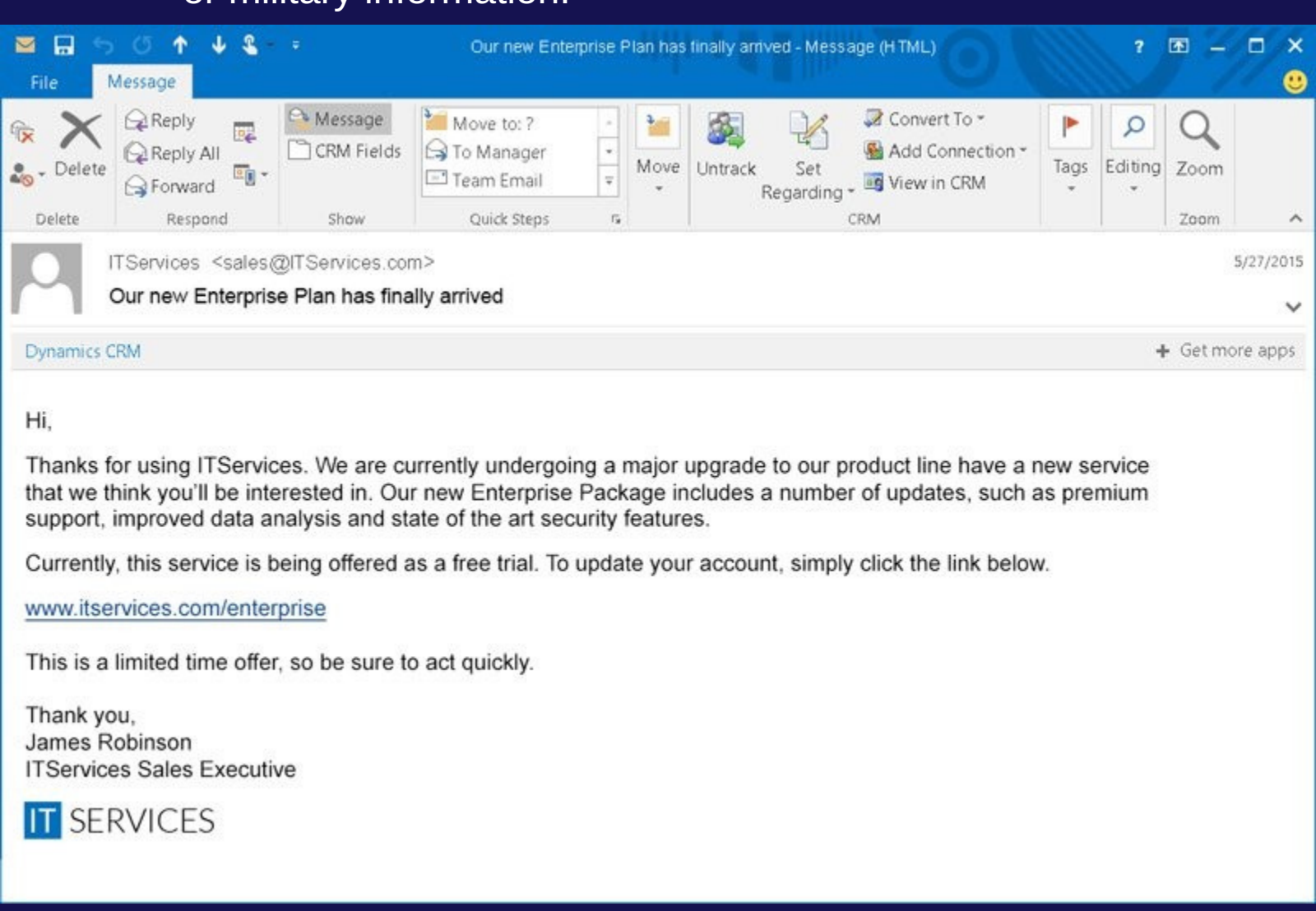
  1-Linking an image directly to the web address and sending it to the victim as a mass email attack.

2-Using an encoded image (.jpeg) or other media files such as .mp3s, .mp4s, or GIF files (.gif). In this type of attack, the Cyberattacker embeds a batch file (.bat) or virus into an image and sends it as an attachment to the intended victim.

- In a voice phishing or vishing attack, the message is orally communicated by the Cyberattacker to the potential victim.

- CEO fraud, also known as Business Email Compromise occurs when the Cyberattacker fools an employee into executing unauthorized wire transfers, or disclosing confidential corporate information and data. More than 70% percent of the scammers pretend to be a CEO. More than 35% percent of these Emails are targeted at financial executives.

- The spear phishing attack is an Email spoofing attack that specifically targets an organization or individual, which aims to get unauthorized access to sensitive information, or other forms of PII. These kinds of Phishing attempts are not typically initiated by random Cyberattackers, but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.



HOW TO AVOID A PHISHING ATTACK

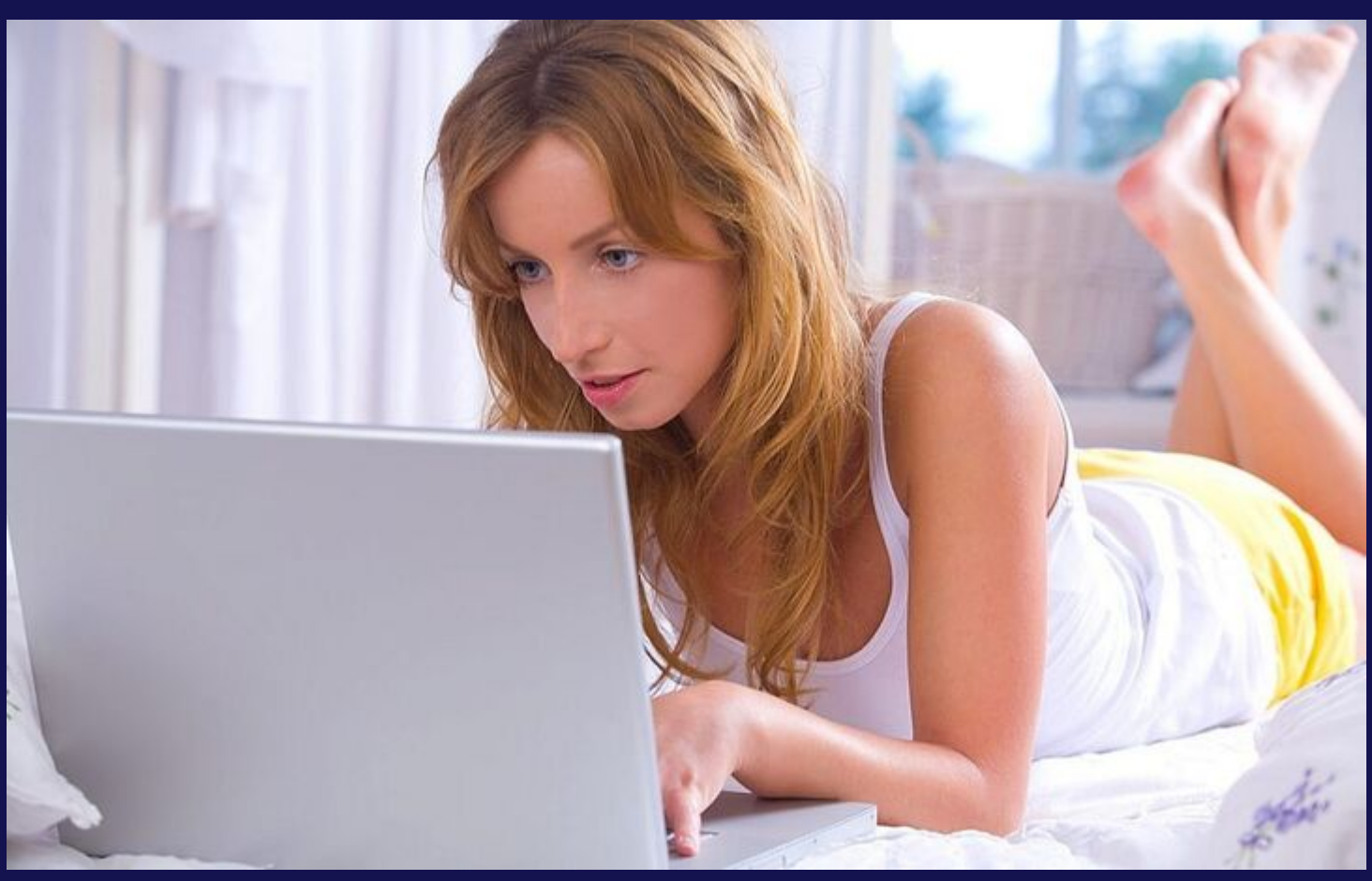
You need to protect yourself from a Phishing Attack from two different perspectives, which are detailed below:

PROTECT YOURSELF!

- Always be proactive before you click! Do not click on links that appear in random emails and instant messages. Always hover over links that you are unsure of before clicking on them. Do they take you where you are supposed to go?
- Make use of an Anti-Phishing Toolbar: These particular toolbars run quick scans on the sites that you visit and compare them to lists of known phishing sites. If you come across upon a malicious site, the toolbar will alert you about it.
- Confirm Website Security: Before submitting your credit card information or PII, make sure the website URL begins with an “https” and there should be a closed lock icon near the address bar.
- Check your online accounts regularly!!! Keep your web browser up to date: Always make sure that you download the latest security patches and updates!
- Be wary of pop-ups: Never click on the “cancel” button; they often direct you to phishing sites. Instead, click the small “x” in the upper corner of the window to close it out.
- Never ever Give Out Personal or financial Information to entities that you do not trust!!!
- Use Antivirus Software: Using firewalls protects you from malicious files entering your network. In turn, antivirus software scans every file which comes to your computer.

PROTECT YOUR BUSINESS!

- Always, always, train your employees to recognize Email scams on a regular basis!!!
- Always use Two Factor Authentication: An example of how Two Factor Authentication (2FA) is that your employee signs in with a password and another form of verification, such as making use of an RSA Token or Biometrics (either Fingerprint Recognition or Iris Recognition).
- Use different passwords: Always have your employees create long and complex passwords, so that they are almost hack proof. In this instance, it is imperative that you make them use a Password Manager.
- Hold mock drills for Phishing attacks: One way to educate your employees is to send them “mock” Phishing Emails. You can always monitor the backend to see if have actually opened the Email, clicked on a malicious link deleted it, or marked it as a spam. These mock Emails will also help you to test the antivirus software applications that are installed on your employees workstations, computers, and wireless devices.



CONCLUSION

We hope you enjoyed reading this newsletter, and looking at the examples of Phishing Emails that we have provided. Remember, although Phishing remains one of the oldest forms of Cyberattacks out there, it is still being widely used and becoming much more sophisticated as new variants of it come out. It is vitally important for you and your business that you stay up to date on the latest trends.

In this regard, one of the best resources to use is this link: https://www.phishing.org/

We also offer a cutting edge service which will help you to avoid Phishing attacks. For more information, click here: http://bluetechcyberincognito.com/

If you have any questions or need any help on how to combat Phishing, please contact us!!!

Sources

1) https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-definition-and-history/#gref

2) http://2.bp.blogspot.com/-7D-0CEuuoH0/U2QIU93BNQI/AAAAAAAAAJ0/lsgjPCVLUXY/s1600/Phishing+attempt+Costco.png

3) https://cofense.com/signs-of-a-phishing-email/

4) https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

5) https://symbolsecurity.com/2019/03/19/how-much-does-a-phishing-attack-cost/

6) https://smallbiztrends.com/2017/08/identify-a-phishing-attack.html

7) https://www.exabytes.com/blog/what-is-phishing-scams/

8) https://www.calyptix.com/top-threats/infographic-phishing-email-attack-flow/

9) https://blog.syscloud.com/types-of-phishing/

10) https://thenextweb.com/contributors/2018/03/23/11-security-strategies-protect-company-phishing-attacks/

11) http://www.phishing.org/10-ways-to-avoid-phishing-scams

12) https://searchsecurity.techtarget.com/definition/spear-phishing