**Intro:**

Cybercrime is only as simple or complex as you can imagine. Unfortunately, cybercrime is on the increase everyday. Cyber criminals are posing more and more threat to individuals and firms. They steal information and identities from individuals and companies for various reasons ranging from financial gains, blackmail and leakage of secrecy, to fame etc.

Cyber criminals always want to be one step ahead. Irrespective of the huge amount of money spent in

Researching & developing “better and more secured” solutions, it is universally accepted and safe to say that no system is 100%s secure. Most at times scammers which may only have fair knowledge of computer security or “hacking” as commonly used captitalise on humans being the weakest link in every system to exploit. That is not to say there are not vulnerable systems.

Cybercrime is actively at the center of most terrorist organisations, hackers aid terrorists to access the dark web to buy weapons and other contraband goods.

**What is cybercrime?**

IBM president and CEO Ginni Rometty described cybercrime as “the greatest threat to every profession, every industry, every company in the world.”

According to ………. cybercrime is any form of criminal activity that is committed on a computer or a network. Usually, the computer is either the object (hacking, spamming) or the target of the crime (hate, crimes, child pornography). The people involved in cybercrimes are known as hackers or cyber criminals.

According to the Council of Europe Convention on Cybercrime, to which the United States is a signatory, cybercrime is a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability, and copyright infringements. However, on a more personal note, cybercrime involves the loss of your information or identity to criminals who use them for financial gains.

**Effects of cybercrime**

With the world increasingly running on data flows, cybercrime vulnerability is also on the rise. Multiple cyber-attacks are reported daily, most of which are automated. Cybercrime has a lot of effects on both companies and individuals as well. Some of the effects are listed below:

1. Security cost: Companies and individuals are spending huge amounts on countermeasures, recovery & insurances.
2. Loss of intellectual properties, trade and business secret
3. Leakage & exposure of Personal information (medical & financial records).
4. Damage to brand name and reputation.
5. Loss of investments and properties.
6. Psychological effects on the victims.
7. Erasure of digital evidence and alteration of data integrity

**Intro**

**What is cyber crimes and shades of cyber crimes**

**Romance Scams**

Preventing romance scams

Researching profiles

Using trackers

**BEC**

**What is BEC**

**Point of entry to corporate emails (tell stories with actual scenarios)**

**-Phishing**

**-Spearphishing**

**-Malware**

**-Dark web data**

**Preventing BEC**

* **Company wide Awareness**
* **Vigilance while surfing and logging in to prevent phishing**
* **Limiting private info on social media to prevent spearphishing**
* **Changing passwords regularly if you’re financially exposed**
* **Using security softwares**
* **Look out for data dumps on the dark web. Change passwords per dump**
* **Using 2FA for logins**
* **Having a standard multi-man protocol for funds transfer and payroll updates**

***Security is never a destination but a process as Cyber Criminals are always trying to be one step ahead.***

Emeka made his primary email public and protected his Google Apps account with a second code that would be sent to his phone – so the hackers got his mobile account.

In February 2020, I applied for a job on a platform. Few weeks later seems the platform was compromised and data stolen, I got a mail from the supposed recruiter. After carefully analyzing the email, I had doubts but the email to have come from a trusted domain. I scheduled a call I was ready to find out who was behind this. The names on the email represented that of the HR which I looked up on several social media sites. But something was just not right… “My suspicion started when plans were made for travelling….

According to Idan Udi Edry, CEO, Trustifi in his article “Why Email is the Biggest Cybersecurity Threat”

***‘‘‘E****mail is the ideal source of all the information a cybercriminal needs and is relatively available due to the carelessness of users. Think about the most recent time you sent sensitive information via email, or better yet, received it.* ***F****inancial information, employee information, or medical records…Think of all the emails you send; would you be okay with those going public?* ***I****magine a malicious cybercriminal gaining access to those emails. Are you aware of the risks, yet still use your dog’s name or your birthdate as part of your password?****’’’***

**Business E-mail Compromise.**

Business email compromise attacks are a form of cyber crime which use email fraud to attack commercial, government and non-profit organizations to achieve a specific outcome which negatively impacts the target organization.

**Point of entry to corporate emails:**

**A. Email’s Point Of Entry:**

It will surprise you to know that one can have access to your email account, have access and possible steal high value data and in some cases completely own the account and by changing login credentials without you handing or sharing your login details with anyone. Let’s take a look at some of the very common causes and ways to gain access to emails.

* 1. Use Of Weak & Easy Passwords: A password may be considered ***weak or easy*** if it is short, doesn’t contain a mixture (of letters, Upper and Lowercase alphabets, and special characters.) A password such as “Adacity“ can be found in the dictionary and a simple dictionary attack will reveal this. “Iwillalwayslovemywife” is quite long a password but Iw!ll@lw@y$l0vemyw!fe may be a better password.
  2. Use Of Same Credentials Across Platforms: Most of the times when one’s social media account is compromised say twitter, user credentials are tried on other accounts by the victim with the hope that the same credentials will grant access.
  3. Dictionary & Brute-Force Attacks: A Dictionary attack is simply an automated testing of login credentials for an account using words or phrases that can be found in the dictionary.

A Brute force attack is simply an automated attack that tries several login credentials from a compile list (password list) of password usually stolen or created from common and default password.

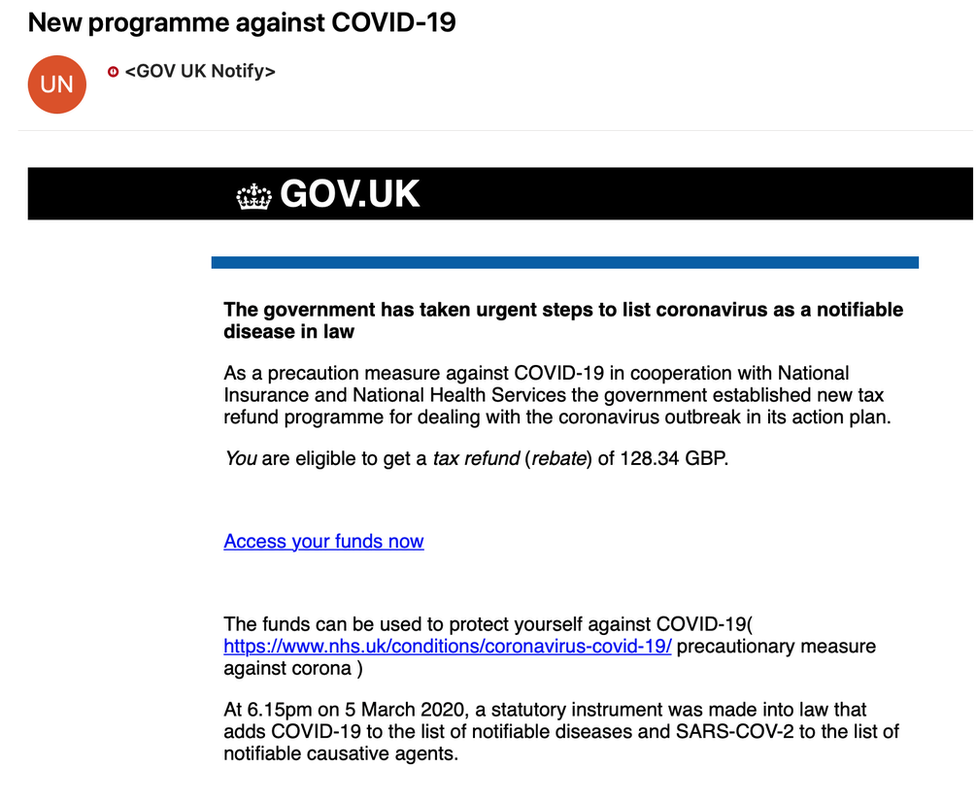
Sometimes your password may not be “simple” but happens to be a password in a password list. When such a password list is used because it contains the right login password access will be granted.

* 1. Use of Social Engineering Principles to Launch Malware Attacks: If you share information or a cybercriminal get cues that you are expecting a mail, response, piece of information a very innocent mail can be drafted to suite this and sent to you. The reader is very likely to engage with the content of such a mail because it was expected.
  2. Unsecure Networks: Using untrusted networks which may not be secured such as public wifi without password for in a bar or coffee shop may cause you more pains than gains. You will be amazed at the amount of information you can

Sometimes cybercriminals which are normal humans also living with us also going about their normal business also can sit close to a bar set up a Wi-Fi network to collect your personal data while connecting you to the internet. It is very key to connect securely to the internet.

B. **Point of entry to corporate emails (tell stories with actual scenarios)**

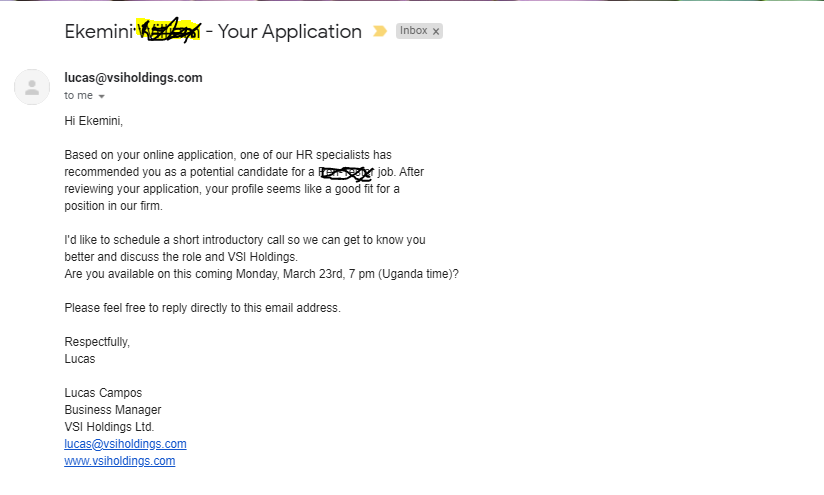
1. **Phishing** is a scam technique that is widely spread and people are knowledgeable about it but yet still fall victim to this regularly. It is the act of faking an email, masquerading as legitimate and most times a well-known company, to fish for passwords and credit card numbers, login details and other important pieces of information. The major aim is to either steal confidential information or for financial gains.



****

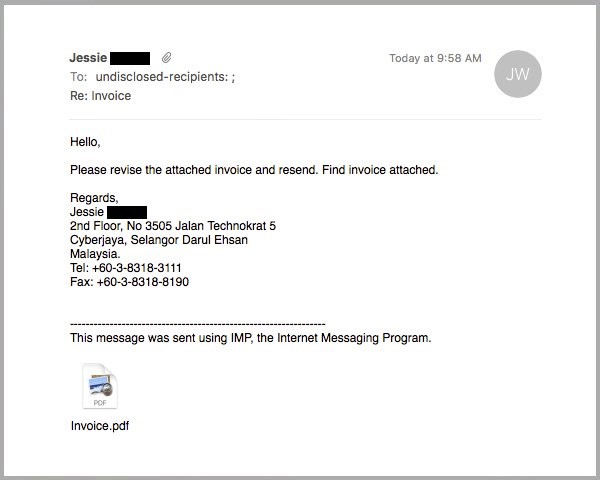
In a time where the world is suffering from global pandemic (Covid-19), with its effect being felt in every facet of life, citizens will love a little financial aid or support of any kind. For this exact reason, this king of email can fly and get reasonable amount of people fall for it.

1. **Spear phishing** emails are carefully designed to get a single recipient to respond. In spear phishing, a hacker identifies a target does enough research about the victim before sending a very convincing or persuasive email. The hacker sends a targeted legitimate looking email, expecting the target to open the email. The Target opens the email containing a malware or a deceptive link redirecting them to where information can be stolen or a malware will be activated.



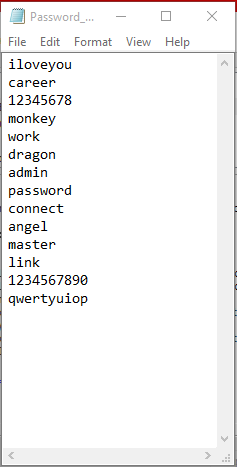
Consider the above email sent from lucas a supposed staff of VSIholdings from the address [lucas@vsiholdings.com](mailto:lucas@vsiholdings.com) as the sender using the domain vsiholdings.com. This email appeared to be legit after and interaction and a careful analysis, it turned out to be a huge scam.

1. **Malware** can be seen as any software intentionally designed to cause damage to a computer, server, client, or computer network. A wide variety of types of malware exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, and scareware. Malware can be disguised and sent as familiar attachment (pdf, word documents, software etc.) to an email. Here a special maliciouscarefully malware was crafted and sent to Jessie, when Jessie was waiting desperately to receive an email in this regards.



1. **Dark Web Data:** The dark web is part of the internet that isn't visible to search engines and requires the use of an anonymizing browser called Tor to be accessed. A lot of activities takes place in the dark web. The dark web is the World Wide Web content that exists on darknets, overlay networks that use the Internet but require specific software, configurations, or authorization to access. So while it's not **illegal** to visit the **Dark Web**, it provides access to **illegal** activities. **Web** sites that exist on the **Dark Web** are encrypted (and thus difficult to track), most commonly through the Tor encryption tool. Therefore, most **Dark Web** users access those sites using the Tor browser.

When there is a data breach, high value data such as (employee data, trade secrets, health & medical records, confidential & personal information, login credentials etc.) are harvested they are usually exposed or sold in the dark web. Login credentials such as username and password in thousands and millions can be sold, the figure below is an extract of a sample password list containing several password which can be used for a brute force attack.



Source: Rapid7

**Preventing BEC:**

* **Company wide Awareness:** It is more than necessary for all the staff of an organisations to get cybersecurity training. Simple periodic workshops, materials, updates on attack strategies will go a long way in saving an organisations from imminent disaster. Not only the technician have to be security aware. This awareness should start from the cleaner to the security man, admin, etc…
* **Vigilance while surfing and logging in to prevent phishing:** Generally surfing the internet can be likened to walking in a lonely unfamiliar street at night. Imagine searching for a job online and submitting all user information to a scam site that uses this to send you a personalized email, the odd of you falling for this is very high.
* **Limiting private info on social media to prevent spearphishing:** I was once able to discuss with a complete stranger, mentioning some deep personal information shared by the stranger years back on social media.***“The Internet never Forget”*** some people jump on social media post & threads just to discuss their pets, mention the places they have been to for vacations, discuss where they live, where they work, the schools they have been to, etc by the time it’s their birthday and year you would have gathered [Birthdate, Address, Pet, Work, ] This is enough to build a password\_list and attempt brute-forcing into their account.
* **Changing passwords regularly if you’re financially exposed:** It is a very good practice to change your passwords, regularly (when you suspect any activity on your account, when there are data breaches on solutions you use or third party solutions. If I have a gmail account which is breached, and it can be used to recover (listed as a recovery option) other email accounts it is safe to change the password.
* **Using security software:** The use of security software such are antivirus on machines etc are underrated that is not t say that malwares do not bypass firewalls and antivirus software.
* **Look out for data dumps on the dark web. Change passwords per dump:** You may not have access to all password or even any dumps available on the internet, but changing passwords each time there is a data breach may also act as a security measure.
* **Using 2FA for logins:** While it may interest one to use 2FA (two factor Authentication), it is advisable to use authenticators such as Google authenticator or any other preferred one as SMS is not reliable and have been compromised a lot of times. Having said that, using 2FA (SMS) is better than not using 2FA at all.
* **Having a standard multi-man protocol for funds transfer and payroll updates:**

**How To Detect A Phishing Email.**

There are dozens of phishing techniques every now and then, but it can also be detectable if you give attention to some of the following factors. It should be note that these techniques are updated frequently

**The email domain & links:**

Phishing emails often use a public domain such as gmail.com whereas no legitimate organization contacts you with such an address. A serious grand Scam will go as far as buy a domain, and having official emails.

However, every organization has its own email domain (the part after the @ symbol) and company account. For example, an email from Paypal will read @paypal.com. If jobs is a staff of paypal and job has an official email from this domain will look like [jobs@paypal.com](mailto:jobs@paypal.com)

You should also know that criminals may also use the spoofed organizational names in the primary part of the email in order to deceive you. The emails are often very similar to the genuine email except that there is always a very minor difference, like replacing an "O" with a zero "0". For example "dragoworks@" and "dragow0rks@"

Hyperlinks makes it very easy to redirect people to other pages if it is a page they are not familiar or have visited before they may have no doubt. A hyperlink is simple a piece of text or image that redirects one to a link (mostly on the internet). It is always wise to hover your mouse over links to ensure where they are leading if you must click.

Click this link [facebook](http://www.facebook.com) to visit chat with friends and this link [mail](http://www.twitter.com) to send us a mail. Notice how the first link led to facebook and the second redirected to twitter imagine if it led to a malware infested domain.

It is also wise to suspect a shortened url. One may want to investigate further.

**Poorly written email**

Most although not all the emails are poorly organized both structure and tone-wise. However, most of the phishing email writing tone, style and structure are always inconsistent compared to the originals. If more attention is paid to the structure of an email, then most of the scam won’t be successful. You may ask, why are the email wrongly type? You should always bear in mind that most of these emails are often sent by persons from non-English speaking countries who do not have a strong command of the language. With the above in mind, you can be able to distinguish a typo error from a legitimate sender and a scammer.

**Suspicious attachments and links**

Emails often contain attachments or a link to a bogus website that may requests login and other sensitive information. The attachments most times, once you download it install a malware that is capable of taking your vital information from your computer. These suspicious links can be uncovered by further investigating.

**Counter Measures & How To Detect A Phishing Email.**

1. There are dozens of phishing techniques every now and then, but it can also be detectable if you give attention to the following factors.

* Learn to research well enough on search engines. A simple search with the right parameters can reveal more than you think
* When an email is sent and you have doubts, call the sender for confirmation.
* Assume the email maybe coming from a legit source but has been compromised halt if you have doubts.
* Look out for generic greetings.
* Avoid emails asking you to act now!
* Beware of online request for personal information.

1. These steps may also useful.

* *Scan Url:*Visit <https://virustotal.com> copy and paste any url or IP address. It guides one’s decision as lots of antivirus and malware solution scan the supplied Ip or url.
* *Investigate IP:* Visit [https://Centralops.net](https://Centralops.com)  or <https://whois.com> to investigate the Ip address. There are several other database to investigate an Ip such as <https://Cyren.com> , <https://whois.net> etc…
* *Contained Environment:* Open attachments in a contained environment so in an event of a malware being sent as an attachment. Visit <https://sandboxie.com>

**How to avoid Phishing & Spear Phishing scams.**

**Stay informed about phishing techniques.**

Being informed about various phishing techniques used by the fraudsters is the first step to take in order to stay ahead of their ploy. It is necessary to be knowledgeable enough to know that, there is a possibility of any email being a phishing email.

**Make sure the site is secure:**

It is common to just log on to any site without first verifying the sites security. To avoid phishing, you should never log on to a site with no http at the beginning. You should also watch out for the locked key symbol on the title bar of most browsers that indicate site security status. Install and keep antivirus software updated in your system.

**Think before you click**

It is not a good habit to always click on any link, as it may totally take you to another site that was designed just for obtaining your details.

**Avoid clicking on pop-ups:**

Make sure to block all pop-ups, but if it manages to infiltrate, avoid clicking on the cancel button as this often lead to a phishing site. It is better to click on the "x" button on the top corner of the pop-up window.

**Use other means of communication to validate urgent requests:**

In an organization, there should be an alternative remote mode of validating vital request in order to stay safe.

**Use anti-virus software:**

Have a working and updated anti-virus in order to protect your computer from phishing malwares.

**Install an anti-phishing software:**

This toolbar runs a background checks on the sites that you're visiting relative to well known phishing sites.