**GREENCORE**

ASSIGNMENT 1

By Dylan Bearman

R00190268

**CONTENT**

* (PAGE 1) INTRODUCTION
* (PAGE 2) CONTENTS
* (PAGE 3) BACKROUND INFORMATION
* (PAGE 4) RANSOMWARE
* (PAGE 5) TREAT ANALYSIS
* (PAGE 6) DDOS
* (PAGE 7) PYTHON
* (PAGE 8) UNAUTHORIZED TRACKING
* (PAGE 9) LOSS OF DATA
* (PAGE 10) REMOTE ACCESS
* (PAGE 11) INFILTRATION OF DATA
* (PAGE 12) FOOTPRINTING
* (PAGE 13) WEAKNESSES
* (PAGE 14) WEAKNESSES
* (PAGE 15) WEAKNESSES
* (PAGE 16) SECURITY POLICU
* (PAGE 17) SOCIAL ENGINEERING
* (PAGE 18) SOCIAL ENGINEERING
* (PAGE 19) HOW TO AVOID ATTACKS
* (PAGE 20) SOCIAL SECURITY
* (PAGE 21) SOURCES

**ABOUT**



Greencore is a convenience food company bringing in 1.5 billion in group revenue and has 15,000 people employed in over 35 locations. The Irish Government have special shares in this company. They are the world’s largest maker of sandwiches, 350,000,000 sandwiches a year and they also have a 37 percent share in the UK Market

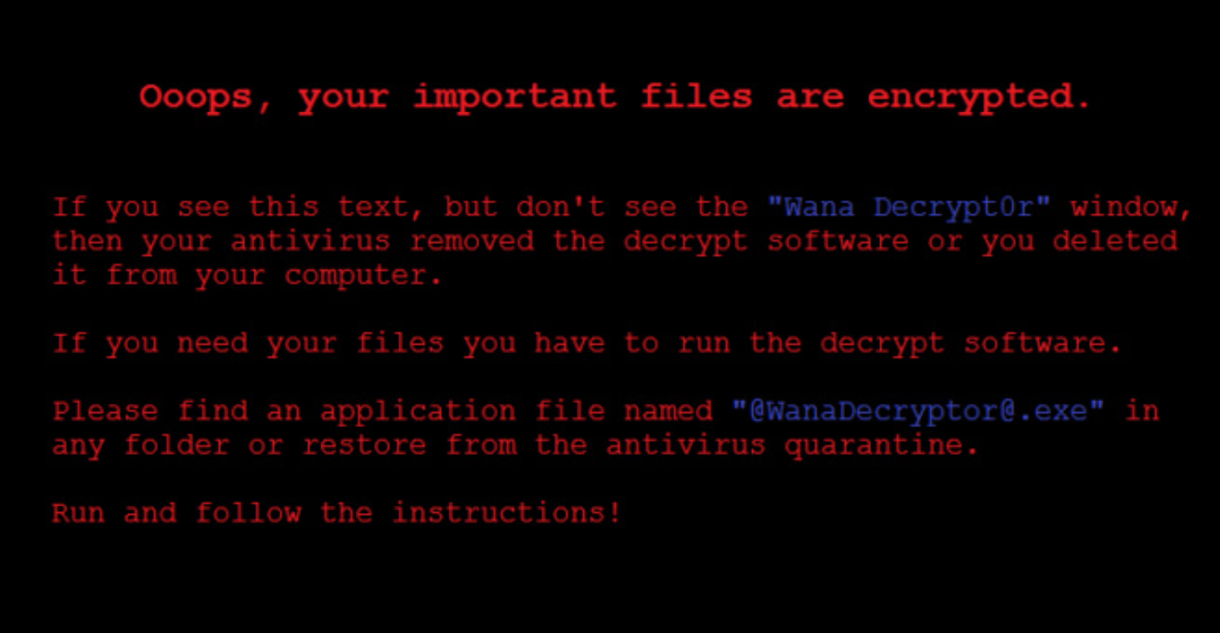
Greencore was originally formed in 1991, it was established by the Irish government following the privatisation of Irish Sugar. Then in 2001 they expanded into convenience food. In 2006 they left the sugar business and the next year they started growing at a rapid rate as there was a strong UK growth through a series of convenience food purchases. In 2008 they entered the US convenience food market with the purchase of Home-Made Brand Foods. Then in 2011 they bought Unit in the UK. The following year they bought HC Shao and Market Fare Foods in the US and International Cuisine in the UK. In 2012 they launched The Greencore way. Then in 2018, Greencore US was sold to Hearthside Food Solutions for 817,000,000 but they carried on trading in all other countries besides the US.

In my opinion this company have a lot of valuable assets, if the wrong hands where to get hold of them it could potentially cost them the business. In my opinion some of their most valuable information aside from cash in the bank would include items like, their secret recipe, distribution routes, batch numbers and customer satisfaction.

**Ransomware**

Ransomware also known as Ransom Malware has been around for years, going back as far as the 1980s where payment was being demanded to be paid by snail mail whereas now it’s a lot more advanced and payments are being made through crypto currency. Once ransomware makes its way to your computer it will start by either locking your computer as a whole or it will lock individual data. You might be wondering to yourself; how does ransomware even make its way to my computer in the first place, well this usually happens without you even realizing what you have done, it could be through an email that was purposely infected with some sort of attachment or some link or a PDF file. The attackers are so advanced now that they use social engineering to fool people into clicking on these links. There are mainly three types of Ransomware, the first being where they lock certain data which they feel holds significant value to who’s computer it is, the second is where they will completely lock you out of your computer and the last and the least significant is where a pop-up banner will alert you of viruses attached on your laptop and they want you to pay to get rid of them. You might say to yourself; how do I get rid of this infectant off my computer without giving in and paying the ransom, well, being honest with you, there isn’t a whole lot you can do, authorities tend to tell people to just pay it as it’s very complicated to get rid of it

**WANNA-CRY**

****One of the most famous examples of ransomware being used is Wanna-Cry.

Wanna-Cry spread rapidly mid-2017. It was infecting window computers and was depending a payment in bitcoin because all the files on the computer had been encrypted. It took advantage of a windows problem that was apparently first detected by the American Government. It has reportedly cost 4billion and it cost the NHS alone over 100 million.

**Treat Analysis**

- [https://nvd.nist.gov](https://nvd.nist.gov/)

-DDos Attack

-Python intrusion

- Unauthorized Tracking

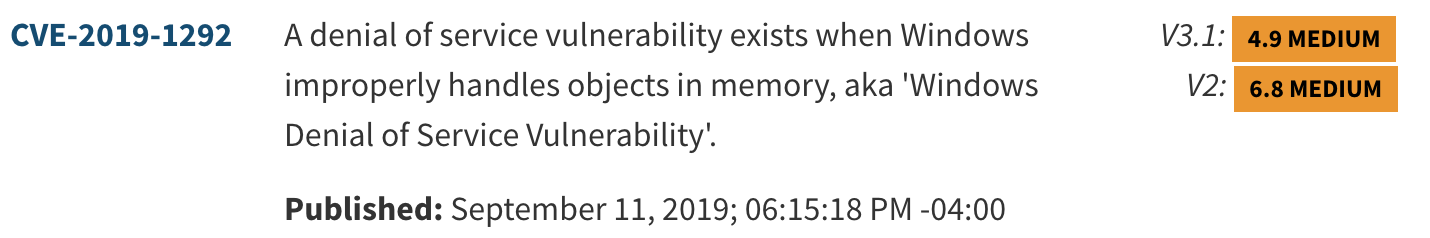
-Loss of data

-https://threatpost.com

-infiltration of data

-remote access

**Digital denial of services (DDos)**



**WHAT IS IT?**

This is a very dangerous threat to any company operating in the 21st century. This threat is aimed at making a network or website unavailable for a certain period. This happens when the attacker sends packets/requests to his chosen person and wipes out their network because it’s filled with billions of these, and it can’t process them and then all the legitimate ones are prevented from being fulfilled.

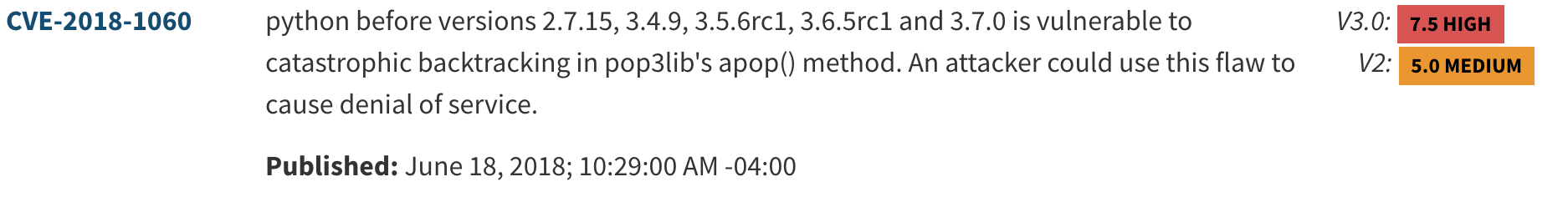
**HOW TO GET RID OF IT?**

The best way to stop a DDos attack is by preventing it from happening. To do this you have to monitor your application traffic continuously.

**THE EFFECT OF THIS ON GREENCORE**

This would have a detrimental effect on greencore as greencores website is used as a communication between the customer and the product and a ddos attack would put a stop to this. It would also have a horrible effect on their network, and this is where they run their business from so it would put them out of action until the attack is resolved.

**PYTHON**



**WHAT IS IT?**

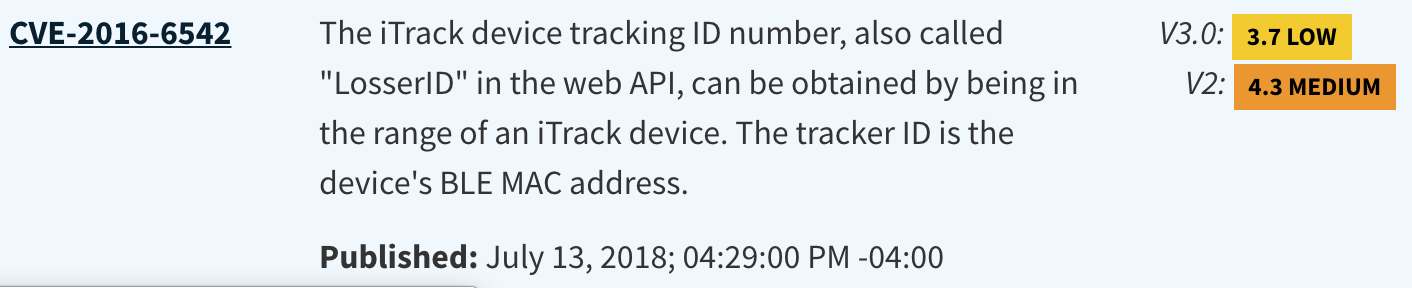
This is also a very dangerous threat to any company operating in the 21st century. Effectively what it is, is that python is vulnerable to catastrophic backtracking and attackers could take advantage of this.

**HOW TO GET RID OF IT?**

All you must do is update python

**THE EFFECT OF THIS ON GREENCORE**

It could potentially run their business as an attacker could penetrate and use this flaw to cause denial of services.

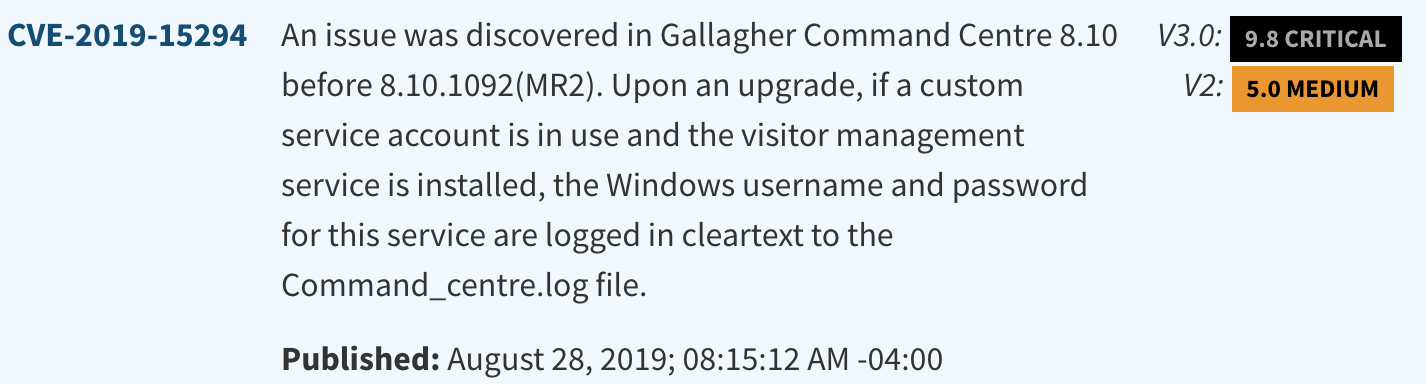
**Unauthorized Tracking**

**WHAT IS IT?** Gives access to an unauthorized person to be apple to track a device in close range.

**HOW TO GET RID OF IT?** It’s as simple as updating

**THE EFFECT OF THIS ON GREENCORE?** It could have giving someone the ability to see a packages location which wouldn’t be good because it would customer and company details on and in it.

**Screen%20Shot%202019-10-20%20at%2022.44.56.png**

**LOSS OF DATA**

**WHAT IS IT** Displayed username and passcode in plain text

**HOW TO GET RID OF IT** There was no fix for it until the system was updated

**HOW COULD THIS EFFECT GREENCORE** Hackers could have remotely seen the passcode for something?

**REMOTE ACCESS**



**WHAT IS IT?**

It’s not that complicated. All it involves is intruders gaining access to your smart device and being able to read your messages but fortunately they cannot respond or do anything else on your phone

**HOW TO GET RID OF IT?**

Once it read, its read. But to stop them from reading future messages you could deactivate your account.

**THE EFFECT OF THIS ON GREENCORE?**

This would have an extremely bad effect on greencore. If someone was able to read messages and if it involved the CEO talking to one of his employees relating to customer’s bank account information or something else vital, then the company could come to a halting stop and wouldn’t be able to trade anymore.

**INFILTRATION OF DATA**



**WHAT IS IT?**

The infiltration of data is when hackers will destroy your system and/or data to cover up their tracks. When I say cover up their tracks what I mean is that their only intention wasn’t to just destroy your system and/or data, that was just a cover so they could have free roam within your company and take data that you have collected without you knowing

**HOW TO PREVENT THIS FROM HAPPENING?**

One of the greatest ways of defending off from hackers when running a company is to hire professional help who have a lot of experience with this type of stuff and employee them full time so they can keep on top of stuff

**THE EFFECT OF THIS ON GREENCORE**

This would also have a detrimental effect on greencore as it could leak information that they wouldn’t want anyone knowing outside of the company. Information that could be included here would be stuff like distribution routes, customer satisfaction and secret recopy.

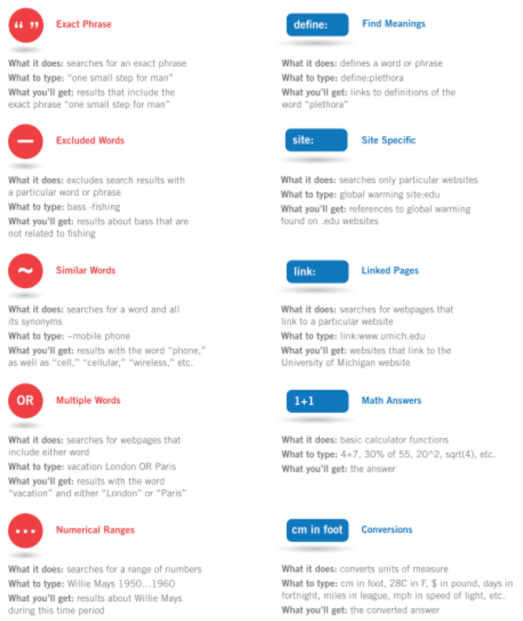
**FOOTPRINTING**

**WHAT IS IT?**

Foot printing also known as “pre-attack” is the way of collecting as much information as you possible can about a specific company and try to find ways to penetrate them. This is what hackers spend most of their time doing before preforming the real attack.

**WHAT METHODS ARE USED AND HOW?**

There are numerous of different way of gathering information about a specific company. These include

****

-Search Engines

Search engines such as internet explorer, Firefox, google chrome can be used to gather a lot of information. When used right it’s a brilliant free way to gather information. When I say used properly, I mean for e.g., if you were looking for the definition of foot printing in google instead of saying “what does foot printing mean”, you could just say “define: foot printing”. Another one would be if you were looking for information on a specific site you could type “what is foot printing site: Wikipedia”. This way it will only bring up information to do with foot printing on Wikipedia

-Web Crawling

Web crawling is another way of gathering information about different people or company’s but with this you’re not confined to a specific search engine, you can use whatever your heart desires

-Whois

Whois is a website with a lot of information. It can provide you with information such as the registration and it can give you email addresses.

-Wayback Machine

The wayback machine captures images of websites going back around 18 years. It can provide with information that someone may no longer want disclosed

-Netcraft

Netcraft is an internet monitoring system and updates us with uptimes and provides server operating system detection and does a lot of other functions

**WEAKNESSES**

**1st WEEKNESS**

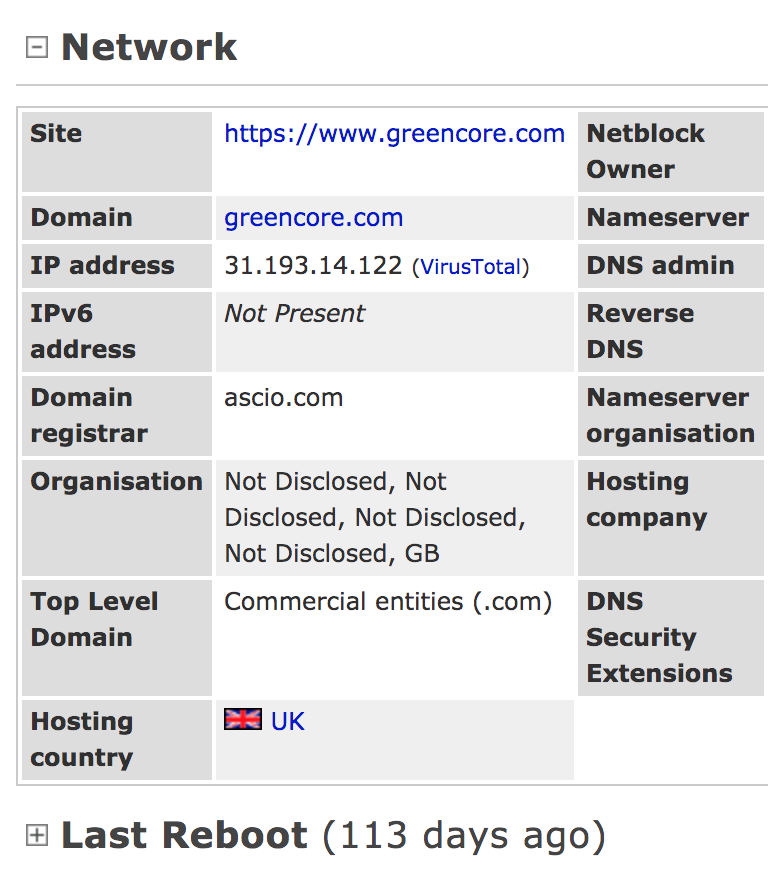
****As seen here they have many locations, one of which in Dublin and the others scattered around the Uk. Once I saw this I became to become a bit concerned for their infrastructure and worried about how secure it was. On further inspection I noticed it wasn’t to secure clearly demonstrated by these two photos. As seen in image one it seems to be a distro centre which would be holding a lot of their stock and unfortunately it backed by a field which is easily accessible from the street.

Again as seen in image 2 it seems to be another distro centre which is backed onto someone’s home. You wouldn’t want anyone suspicious living here would you

****

This is extremely dangerous. Its not a good idea having their infrastructure this unsecure. Especially where they keep their stock. Because at the end of the day this is how they make their money. There are a few ways they could improve. One would be t fence the perimeter on the distro centres. Another would be to implement the system that I talk about at the end of task 2 or finally they could move but it would be very time consuming and it would waste a lot of resources.

**2nd WEEKNESS**

****

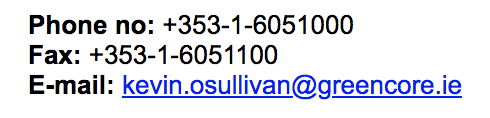
When I enter the domain “greencore.com” into the netcraft toolbar I get a lot of useful information, along with this information is the fact that the network hasn’t been rebooted for 113 days. Sometimes rebooting is necessary when installing a new software or installing a new operating system or even for stuff just as small as fixing minor errors. When it hasn’t been done for 113 days that shows something is wrong, if someone was trying to break into greencore this would be like Christmas to them. There’s a simple fix for this as swell and that is to just reboot the system

**3rd Weakness**

**Screen%20Shot%202019-10-20%20at%2023.07.42.png**

On whois we have managed to obtain the ip address of the server. With this we now have a place to send all our packets to if we would want to Ddos them. There is a simple fix to this and that is to have a bouncing ip address. That is one that changes every so often

**4th Weakness**

****

On the way back machine I found contact information belonging to an Irish civilian Kevin O Sullivan. I’m not too sure if he would be too happy with that information getting out now.

**SECURITY POLICY**

In my opinion a company security policy should extend to social networking and other uses of the internet. I say this because social media can be a very dangerous tool for hackers. There are so many threats that could take place to a company through an employee’s social media.

For e.g., let’s just say you decided to post that you and your office were going on a 2-day trip from Thursday to Friday. After you click post on this you have effectively just told the world, no one will be in the office for fourth eight hours straight, feel free to break into the office and plug in key loggers into all our computers, install hiding cameras around the place, remotely tap into our WIFI network.

It just doesn’t make sense. The same way if you were going on holiday you don’t put a note up on your front door saying, not home for the following two weeks, please call me if its urgent.

It’s reported that only 51 percent of companies have a social security policy. It said that a social security policy is just as important as other policy’s such as discrimination and stealing.

70 percent of working reportedly use social media while at work and 50 per cent of these say they use it for at least an hour in the day.

Using social media at work has many downfalls. A few of these include speaking badly for the organization you’re working for, being victim to online scams and because of this malicious software has been downloaded to your work computer. Finally, and the most important of them all is the possibility of hackers breaching the system.

**SOCIAL ENGINEERING**

**WHAT IS IT?**

Effectively social engineering is retrieving confidential information from a person without them even realising what has happened. The information the criminals are looking for can change depending on the circumstances but for the most part they are looking for bank details, your passwords or even access to a computer so they can download malicious software that will later give them access to your computer. Sometimes they may not even need access to the computer but all they would need is access to the physical computer and they can install a device called a “key logger”.

Social engineering is preferred over “hacking” for criminals because it is a lot easier, for e.g., it’s easier to have a conversation with someone and try drag their password out of them then it would be to try hack their password.

If you were to ask any security professionals, they would tell you that the downfall in any security protocol relates to the human.

**WHAT DO THESE ATTACKS LOOK LIKE?**

These attacks come in many shapes and forms, I could list these attacks and I’d never finish because there are so many places they can attack and there are so many possibilities as to how they will conduct the attack. For today I’m going to give you a detailed description on some of the main ones that happen very frequently

1. **KEY LOGGERS**



What is a key logger you may ask yourself? Basically, it is a small little black device that plugs into your computer through the usb slots and then your keyboard plugs into the back of this device. The point of this device is that it logs every button you have pressed on your computer accompanied with the times they were pressed at and it stores this information on the device until it can access a valid WIFI network, once it makes contact with the network it will upload the information and the hacker on the other side can download this information and more times than not you would have entered the passcode to your computer, maybe your bank details and possibly your social accounts. How this related to social engineering is the fact of how the “key logger” got access to the computer. Well, that’s the whole point, for the device to have been able to be plugged in someone must have given this not so trustworthy civilian access to the computers within the business.

1. **EMAIL FROM FAMILY**

If the hacker manages to gain access to your email either through social engineering or just by hacking into it, he will have access to all your contacts and being honest with you he will more than likely to have access to most websites, you use online seeing as nowadays everyone uses the same passcodes for all the different 10 accounts, they use including their bank website. Once they have access of the email, they will send emails out to the friend of this person. All these emails will either contain a link or a download, both the link and the download have malicious software downloaded onto them so that as soon as you press on the link or press the download you will become infected, and they will be able to retrieve more personal information off you then.

1. **PHISHING EMAIL**

A phishing email is one where the hackers send you an email that looks like it has come from a reputable source and ask you to fill in some sensitive information. Once you have filled in this information it will be sent straight to the hackers and then they will have free will with what they choose to do with it

1. **CONVERSATIONS**

In recent years we have seen them bring in so many rules and regulations relating to the general data protection. You may ask yourself why they are doing all this. Well, this is being done because there have been millions of cases where sensitive data gets leaked to the wrong person. How they do this is just unbelievable, no ‘hacker tools’ needed or anything like that. All they do is for e.g., they will ring up your phone provider, at this point all they have is your name, and with this they may find out what your email address is and once they have this, they will be giving access to reset your passcode. How they are giving access to your passcode reset could be by providing another small bit of information that will convince the person on the other end of the phone that the person they are talking to is you and then they can do what they want. They might also play some background noises that in a way ‘forces’ the person to hand over information because she may get emotionally attached.

**HOW TO AVOID ATTACKS**

1. **HOW TO AVOID DIGITAL ATTACKS**

**-THINK BEFORE YOU ACT**

The hackers want you to act before you think, but that is never good. The best practise is to stop and think to yourself. Does this message seem like I must act quickly either with nerves or excitement? If you seem a bit unsure the best option is just to leave it be and delete whatever it may be. If the message was really that important, I’m sure you will hear back from that person or company again on a later stage

**-PASSWORDS**

I know this may seem a bit too simple but never keep the same two passcodes for different sites or never keep a passcode active for a long period of time. If the hackers somehow gain access to one of your passcodes and if every other passcode you have is the same then before you know it, they have access to your bank details, credit card information and any other sensitive information you may have.

**-DOWNLOADS**

If you receive an email from some that you don’t know that contains a link to download something more than likely it isn’t what you think it is.

**-LINKS**

Like the downloads, if you receive a message and it contains a link that looks suspicious your best option is to just leave it.

1. **HOW TO AVOID PHYSICAL ATTACKS**

More times than not physical attacks involve someone gaining physical access to your computer with the company, someone having a general conversation with you trying to squeeze out as much information as possible or someone gaining access to your company building with authorisation and seeing little snippets of information that will help them.

**-THINK BEFORE YOU ACT**

Similarly, to preventing digital attacks, when preventing physical attacks one thing to do is to think before you act. If someone that you don’t recognize walks into your building wearing a high-vis jacket without any credentials, the best thing to do is to question them rather than letting them wonder where they went. Another example would be if someone came in and said that they were there to inspect the computers and fix the, escort them to wear they need to be but at the same time don’t leave them out of your site.

**-VERIFICATION**

Always verify that the person is who they say they are before giving them access.

**MY RECOMMENDATION AROUND WHAT AUTHENTICATION SYSTEM SHOULD BE IMPLEMENTED TO PREVENT PHYSICAL ACCESS**

In my opinion the best system that prevents physical access from the outside would be a key card system. I know this is common practise nowadays but most of them have doors around the back that aren’t restricted, and they aren’t locked either. A lot of them are also very generic, what I mean by this is that one key card gives you access to the entire building

The sort of system that I think would suit best would have a lot of different areas to cover.

1. The first way to approaching this system is by installing a system that only allows you access with a key card on every single outside door of the building except the main entrance. Now we have every outside door covered.
2. The next thing to do is to make sure that all the windows around the perimeter can be locked. By now we have covered the outside of the building beside the main entrance which is wide open to the public. But this isn’t a problem. We just must make sure that no sensitive information is lying around. We also must make sure that there are no ports in the main entrance which would allow someone from the outside to gain access.
3. Now we must put one of these systems that only allows access with a key card on every single door within the building.
4. Once step 3 is done we can start getting a list of everyone whose employed within the company and restrict them from gaining access to places they shouldn’t be able to.
5. Now we have most of it done but what would happen if a visitor was to visit. Now we must create a system that allows someone with top level clearance to be giving the opportunity to create a visitor’s key card when needed and to be able to customize it depending on where they need to be.

With this system I have created everywhere is restricted and only certain people have access to certain places. If someone were to visit, there would be someone available to print them off a key card and customize it to their liking. If in the worst circumstances something was to go wrong and data leaked, they would be able to see who is in what room and every moment and they would be able to locate where the breach came from

**SOURCES**

* www.greencore.com
* [www.web.archive.org](http://www.web.archive.org)
* [www.whois.com](http://www.whois.com)
* [www.netcraft.com](http://www.netcraft.com)
* [www.google.com](http://www.google.com)
* www.dato.com
* [www.cisco.com](http://www.cisco.com)
* [www.webroot.com](http://www.webroot.com)
* [www.greycampus.com](http://www.greycampus.com)
* [www.icann.org](http://www.icann.org)
* [www.tech2integrate.wordpress.com](http://www.tech2integrate.wordpress.com)
* [www.raymond.cc](http://www.raymond.cc)
* [www.geeksforgeeks.org](http://www.geeksforgeeks.org)
* [www.nvd.nist.gov](http://www.nvd.nist.gov)
* [www.csoonline.com](http://www.csoonline.com)
* [www.techrepublic.com](http://www.techrepublic.com)
* [www.enteprise.comodo.com](http://www.enteprise.comodo.com)
* www.network.information.com