Avon and Somerset Police
SERVE. PROTECT. RESPECT.

COVID19 PRESENTATION & GUIDANCE DOCUMENTATION

Contents

Avon and Somerset Police
SERVE. PROTECT. RESPECT.

Introduction

I am Kristian Evans, I work for Avon and Somerset Constabulary as a Cyber Protect Officer. Due to the Crisis of Coronavirus, I am unable to give talks and presentations in person for the events that have been planned. Therefore, I have produced this information pack for you to read and refer to during self-isolation, which is the advice given by the UK government. With the increase of people working from home (WFH), there is a much greater risk of cyber threats occurring, including ransomware attacks, phishing attacks, and online fraud. In this document I will also cover who to effectively work from home safely and securely.

I will be writing this document in-line with the presentation and make it easy to follow by using numbers in brackets e.g. (1) to identify the slide/page number relating to the presentation. If you have any questions or need more information on any of these topics, please contact me: Kristian.evans@avonandsomerset.police.uk

Sources

I would like to start this document with some of the most important websites to refer to with looking for advice about any cyber related information on Coronavirus. Some will also provide other information useful information which is not related to cyber or the Coronavirus. These websites are as follows:

- Action Fraud
- National Cyber Security Centre
- National Crime Agency
- South West Regional Cyber Crime Unit
- Cyber Aware
- UK safer Internet Centre
- Take Five
- Government Website
- How to geek
- Lifewire

When looking for advice of any category about the Coronavirus pandemic, you should always be referring to the factual sites, such as the list above. This is because social media and other platforms can easily be misinterpreted by people in which they are read and wrote. Therefore, it is essential that only the true facts by official sites should be regarded as true.

Avon and Somerset Police
SERVE. PROTECT. RESPECT.

Background Information – COVID19

As you can see from reading the information on the image in the slide (5), there has been a substantial increase in Coronavirus-themed scams, with over 400% increase by March. The total current loss at the time of the image is £970,000. This is a huge amount of money lost in the time scale.

On the image there are some tips that you may want to follow when working from home during the outbreak. They will save you and your employer from disaster and potential financial loss. Please take a moment to read them.

In the next slide (6), there are a few examples of the types of scams out there that are currently trending. These are people selling "face masks" at discounted prices, masquerading as the World Health Organisation (WHO) asking for donations, and emails impersonating official government websites saying that you are eligible for a "tax refund".

All of these are scams or phishing techniques that draw you in and eventually exploit your human nature to react or create a sense of fear/urgency. They are all fake! I will cover Phishing later in the document.

Ransomware – Case Study

(8) Has anyone heard of WannaCry? I'm sure you have if you were watching the news in in May 2017. This was an attack known as ransomware, which essentially encrypts all data and information on a computer in the background and ultimately asks the user for money to return the files to their original state. To add to the severity of the situation, the cybercriminals will give you a time limit and if the ransom is not received in time the price will drastically go up or they will threaten to destroy the data, trying to create panic forcing you pay the cybercriminals. We don't endorse you paying but ultimately, it is your decision.

WHY?

This is because you cannot guarantee that those files that have been stolen and encrypted by the attackers will be returned. The most likely case is that they have be looking for vulnerable candidates who respond and make even more money by saying they "changed their mind and want more money". This could effectively go on forever, due to the attackers using the information that is important and threatening it all being released to the public or press unless you pay them not to release the information. However, most cyber criminals will destroy the data or return the data but in a modified way. Modified data may leave you with a returning attacker in the future.

Slide (9) displays some of the recent ransomware attacks that have been release in the media. These attacks are vastly targeting businesses, charities, schools, and entire cities. If you think it won't happen to you, you are wrong.

WannaCry Information

This was a ransomware attack which is most well-known because it hit the NHS causing major disruption to medical services, 19,000 cancelled appointments, operations etc. It's also about as close as computer-nerds can get to a coolish story. WannaCry is a strain of ransomware. Like many packages it is actually part of a compound set of different exploits that are engineered together by sophisticated specialists In this case it was linked to a North Korean Group called 'Lazarus'. This highlights how mainstream Cyber is now in international relations. Because the cost of entry is very low it allows countries which are unlikely to have the finance and skills to develop an Aircraft Carrier to get in the game if they can afford a few very expert computer engineers. You can cause far more damage at low cost from anywhere in the world using cyber weapons.

The attack famously hit the NHS but it was part of a much wider spike of incidents that hit loads of end users. In our area the Regional Cyber Crime Unit worked with a medium-sized family firm who had been hit. Notably the initial suspicions arose because a customer noted that an invoice they had received didn't feature the company logo, the reason being that this was generated by the company server which had been compromised which highlight the importance of being aware and reporting things which look odd across an organisation. The company had 200,000 files encrypted including invoices, product info, receipts and the like. The company had no anti-virus, no firewall and their server hadn't received any updates for 6 months and the only reason they managed to recover was because they had sufficient back-ups to restore their critical files.

Vulnerabilities and Protection

(10) Now you have an insight to the destruction ransomware can create on a computer or network, you don't have to be a sitting duck and become a victim to such an attack. I would like to say that you can never be 100% secure, it is impossible due to the ever changing attack vectors and new vulnerabilities. However, you can mitigate the potential to become a victim of such an attack. If you take preventative measures to secure the gates, the attackers will leave and find an easier and more vulnerable target.

Below is the necessary steps to take in order for you be secure online, protect against phishing attacks and being a victim of ransomware. I also would like to add that most of the information is seen as good practice for any attack to do with cyber, as they can all be related to each other in one way or another.

Avon and Somerset Police
SERVE. PROTECT. RESPECT.

Protecting your Credentials - Passwords

Before continuing reading this section, check how strong your password is here and see how weak or strong your password really is and how fast it can be broken by a cybercriminal.

On Slide (11) is some of the most common used passwords but this is not all of them. The list is very long and there are too many to put on the slide. You can google the "most common used passwords" to see them.

If you did check your password on "howsecureismypassword.net" you probably had your password broken within a shocking amount of time. Those who think their password was secure by using numbers, Capitals and/or special characters and still had their password cracked within seconds or a few minutes, this is because the algorithm behind the attackers tools are extremely sophisticated and can be conjured by common things like, activities, events, films, series, etc. and put into a list to attack and locate your password. This is a real eye-opener of a website. Think of another password now and input it into the website and see how long it takes to crack.

Another point to add is that if you use numbers or names (so anything relating to you) the cybercriminals will generate a "dictionary" and use that to brute force/attack your password. This information can easily be gathered covertly by using the internet search engines or people's social media profiles.

So, you might be asking, what is a good password?

It is advised that you create a complex password that is difficult to crack but easy to remember. In order to do this it is recommended that you use three (3) random words. For example, ConcreteOceanKettle. All these words are random and do not link with each other. After checking the password security level online, it would take 318 trillion years to crack.

A second secure password is a passphrase. This is where you create a sentence of words and take the first letter or some of the letters. For example, HmnisKR.IbmfcI2002, which means "Hi my name is Kris [.] I bought my first car in 2002". The idea is to make it appear random but only you know that it actually means something and making a complex password easy to remember. This password word take 18 quadrillion years to crack, which is insane. These passwords are deemed to be the best and I advise you to use them. Additionally, you can add to the complexity of the passwords by adding symbols to the password where it suits you.

Protecting your Credentials – Has your personal information been leaked?

(13) Data breaches happen almost every day, once these get reported, they then are added to a database. You can search online for "have I been pwned" and input your email address to find out if

your email has been linked with any data leaks from companies and businesses. For example, the most recent data breach was the “My Fitness Pal” and although my password was extremely strong, the password still was leaked through weak security in the database that was storing the information. This is way you can never be 100% secure. Attackers will try to find another root to exposing passwords once you take the precautions of having a secure password. Check if your email has been in a data breach and make sure you change your password if you have.

Protecting your Credentials – Password Managers

(14) A password manager is another alternative method to securing all of your daily passwords. These password databases securely store passwords and other personal information, such as bank details, notes and addresses. Some of the password managers use extensions within the browser like Chrome or Firefox. When creating passwords in these managers you can either create one yourself or have the password manager randomly generate one for you. This generated password can be extremely long and complex but you don’t need to remember it, the manager does it for you.

However, you will have to remember one password in order to get into the password manager. This password is known as a “Master Password”, which should be the strongest password you can possibly think of because if this password is broken the attacker will have access to all the other passwords and any other information stored in the manager. So, do not use your partner’s, children’s or dog’s name!

These passwords managers can be accessed across all devices and some are free, some have more features like multiple accounts. These are usually paid as a monthly membership fees. In addition, the better password managers will have you enable two-factor authentication for recovery purposes, if you get locked out of the account. I’ll talk more on this in the next section. I personally use 1Password but I have also used KeePass and LastPass, which are free.

Protecting your Credentials – Two-factor Authentication

(15) Finally, on protecting your credentials, providing Two-factor authentication (2FA) on you accounts will provide added security by adding another layer of security in order to access an account. Therefore, even if you have an extremely strong password and it has been in a data breach, the cybercriminals need to pass the second stage to have access to the account, which is authentication. This is usually done via a code that is sent to your mobile phone number, which you then enter and gain access to the account. Another method is using a smart phone and accepting an authentication notification on an app provided by the company (i.e. Google authenticator or Microsoft authenticator). It is known as 2FA because you verify the account with a password and then authenticate you are who you say you are by providing a code from a device that the account holder owns and setup when the account was created. Therefore, the recommendation is to set up 2FA wherever it is available. Most of the company’s applications today support 2FA.

(16) It is highly recommended to use 2FA for the most important accounts, such as banking, social media, and email accounts. This is because these account can be highly attractive to cybercriminals because they can manipulate other accounts or you as a person if they get hold of any of them. There are some examples of 2FA applications on Slide (16).

Mobile Devices

The next stage is to secure your smart phones. On the slide (17) shows a list of how you might secure your phone. It is very similar to any other device but with a few additions, such as remote wipe, geo-location services to find a lost device, and app stores like Google Play and Apple's App Store.

Try your best not to lose your device as this is one of the most important tools accessing accounts, it is very annoying and difficult to set up all your 2FA to another device but it can be done. I speak from experience.

Again, make sure you have a strong password to get into the device. It is recommended not to use a PIN number because people usually put their date of birth. If you are going to use a PIN make sure it is something that is not your D.O.B and use the maximum amount of digits available.

Enable find my phone applications, so if you lose your phone you have a chance to find it again or can use the information and report it to the local authorities. Enable cloud back up in order to save you information in the Cloud. If you lose your phone any information on the device is stored in the cloud, which can be downloaded to a new device at a later date. You should also enable to ability to remote wipe the phone because, if lost, you can lock the phone and wipe all the data on it, keeping the integrity of the data, if it was to be accessed by someone who should not.

You can also add password managers to your phone by downloading it from the stores. This will keep all your passwords safe from attackers or unauthorised people from accessing your accounts if they got into your phone because they would need the "master password" to access those passwords. Additionally, the password managers usually lock after a short period of inactivity.

It is advised that you use only trusted app stores like Google Pay or Apple's App Store because they provide a built in layer of security and audit the applications that companies want to advertise on their stores. Only a successful audit can allow their product to be available for download because they met the required criteria.

Avon and Somerset Police
SERVE. PROTECT. RESPECT.

Firewalls, Software Updates & Antivirus

(18) Now we are going to talk about some more of the technical measures, these are essential for keeping devices secure and protecting your device from cyber-attacks.

Firewalls

(19) Imagine a castle. You could pull up the draw-bridge, fill up the moat and never let anyone in or out. This is useful if you just want to protect your treasure and never intend to spend it or add to it or otherwise have to come in or go out of your castle. At some point most people want to use the castle to function as part of a wider community and so, you lower the drawbridge. This is your connection to the outside world.

Now you're at risk of people getting in and stealing your treasure, burning your food-supplies and embarking on general pillaging so you create some rules about who can come in and go out. You probably let anyone out as that's less of a security risk. Although you might want to check they don't leave with suspicious looking sacks jingling on the way out. You might say the butcher and leatherworker can come in if they have a signed invite, the baker can only come in on Tuesdays, the fishmonger can come in whenever she likes and the village idiot is never allowed in because we know he'll wreck the joint. This set of rules is given to the gate-guard and this becomes your firewall. You want a guard on duty with this set of rules.

Now every so often, despite the best efforts of your castle engineer, you may find that there are cracks in your castle security that can be used to get in. Ladder engineers design a bigger ladder that can reach over the moat to the tower window, the drains that pump sewage into the moat can actually be crawled through by a small person who could then change the rules on the gate, so that the village idiot is allowed in next time. Now a good castle engineer provides continuing after-care, so that as soon as they notice these new vulnerabilities they will come around and fix them – board up the tower window, put a grill on the sewage pipe. This is your software updates.

Even with the best and regularly patched castle security system attackers may still get in, either through a vulnerability that hasn't been patched or because they got through disguised as the fishmonger or maybe told the butcher to carry some ropes in for them and hang them over the side of the wall. What you need is someone by the gate saying – why is the butcher carrying 2 bags and a rope that's not what the butcher usually brings in, why is the baker's boy trying the locks on the door to the big tower that's not how he should behave, and before castle Grayskull was robbed a small boy was seen checking the locks to their big tower. And then they grab the baker's boy by the ear and slink him in the moat. That's your Anti-Virus, constantly slinging baker's boys into the moat.

In most cases the firewall will already be on. However, if it is not, turn it on. It is the security perimeter of the network. It could be the defence that could stopped an attack that should never have happened. In slide (20) there is a visual representation of how a firewall is implemented in a

network. You have the computers that connect to the router, the router has a firewall built into the device, which then allows or denies your requests to the internet, ultimately displaying the request webpage you are after. Please take a moment and refer to it.

Antivirus/Anti-malware

(21) Antivirus and anti-malware is exactly what it is, protection from viruses and malware. These are computer code that exploits a vulnerability with the system, which could be anything from applications to the hardware being used by the system. These are the defences that must be enabled on a device at all costs. If they are not, how do you know if you are protected and your computer is not working for or reporting to another computer over the internet? This is where the antivirus comes in by scanning the traffic incoming and outgoing over the internet and on the system locally.

An example of a virus was the ILOVEYOU virus was from the early days - back in 2000. But this is before the explosion of the internet and the degree of internet security that exists now. Basically it send an email saying I love you with an attachment love letter, which of course everyone opened. It then spawned itself to everyone in your address book and replaced all your media files with a copy of itself. Now 90% of all emails are spam. A bit annoying for you as an individual yes, but the cost was estimated to be over $15bn when you take into account the crippling of email servers in all the businesses affected, loss of service, loss of files etc.

So, in slide (22) there are some antivirus and anti-malware companies out there offering protection to your computer. These are mostly paid subscriptions but some can offer limited free versions. Do your research on what they offer differently and what suits you best before making a purchase.

However, most computer like Windows offer a free antivirus software, at a basic level, which can be turned on in the settings. On Windows, this software is Windows Defender. So, my suggestion here is that if you are using multiple devices then third party protection is what you should go for because they usually offer the ability to use the product code on more than one device. Plus, they are generally more secure because they offer more than just the basic security and it is their job to be secure.

Software Updates

(23) At this point I am going to relate back to the ransomware attack that happened on the NHS – WannaCry. This attack was very significant and hit networks worldwide but there is an interesting chain of events before it was seen in the wild. WannaCry in the end is just ransomware, which

encrypts your data on the hard drives of the machine and on the network meaning that you cannot use them until you get the decryption key, which usually involves a payment – a ransom.

I won't get into the details of how the ransomware attack happened but essentially someone opened an attachment that launched a program that was vulnerable to an attack, which reported back to a server, which ultimately downloaded the ransomware on to the machines across the network and infrastructure. The most disappointing thing about the attack, for all those affected, was that Windows actually deployed a patch to update and secure the vulnerability that caused the attack in March 2017 and the attack happened in May 2017. Therefore, the attack could have been prevented if they had updated the operating system (Windows environment). This is why it is essential for you to update any device with the latest patches, you can even get new features for the application too, so why not just do it?

Backing Up

(24) We mentioned backing up your phone and we recommend doing it for your other devices too. This is because if it breaks or you lose it you can recovery the data and install it onto another device. Backing up is an essential Cyber Security activity and should be undertaken by all. With reference to the ransomware attack on the NHS, when the data is encrypted and the only way to get it back to its original state is buy paying a fee. In reality, it is advised to never pay the ransom because you may never actually get the information back or you might not have enough money to pay for the decryption key. Therefore, being able to reinstall the operating system from scratch and importing the lost data from a backup is a much more cost-effective way of restoring the system before the attack occurred.

There are generally two types of backups. The first type is a backup of all of your important files and data that's on another hard drive. This enables you to easily import your critical data onto another drive if the one that is currently being used is stolen or gets corrupted. This drive should not be connected to the computer permanently.

The second type is a full system back up. This takes a backup of the current state of the system and will include the operating system. These generally will come at a price but are the most secure way to back up your system and it will have every file, document and information in the snapshot.

As for file backup options, you can use Cloud storage or physical storage that is not attached to the system after the backup is complete. The recommended root is through Cloud storage because the backup is not in the same vicinity as the computer and you cannot be responsible for losing the data. However, they might come at a price if you have a large amount of data to backup. Options of cloud storage can be from most of the big vendors, such as Google, Microsoft, and Dropbox. On the other

hand, an external hard drive is much cheaper but you are responsible for the device, if it is lost so is all of your data.

If you use your search engine for “Cloud storage” a list of websites will appear. The main ones are usually, iCloud, Google Drive, Dropbox, and OneDrive. Some of these vendors supply a limited amount of storage for free, which is like a “free trial” for you to test the reliability of the product and how it works. Others we require you to pay and they all have different data plans available.

Reporting

(25) I would like to take this time in the presentation to inform you that if you have been a victim of a ransomware attack, please report it to Action Fraud because then we can see how the attack works and what devices it is affecting, any information can help to catch the cybercriminals behind the attack. Furthermore, Action Fraud is there for support of any other fraud-related crimes. They will help and support you through the events and provide guidance on what to do.

Phishing during the Outbreak

(26) So, I’m sure by now that you have heard of the term phishing floating around. It gets its name from the notion that the attacker dangles a hook with some bait in the hope you’ll take it. There are various forms of phishing and they all have different names. However, I’ll keep it simple, the main phish can be carried out over text message, voice calls, email or social media. The majority of the hooks will be in an email with an attachment or link for you to interact with. The links will either take you to a fake website from where the attacker will try to infect your computer or get you to enter your personal information, or the link might be a program that you start from the moment you click it.

On the other hand, attachments in emails often have some hidden code within the application that is being run – opening a word document – upon opening the attachment will start the chain reaction of the code to be executed by the computer and infecting your machine. Alternatively, the phish might get you to hand over your credentials in some way. For example, making an urgent request to update your information because of “xyz”.

(27) Phishing works because people are inclined to react to helpful, social instances or you might lose out. People tend to fall for these attacks people are being nice or there is something to be gained from helping. People want to present themselves as “helpful” to new people and potential customers. However, this could be more damaging than “helpful”. Once the attacker has got you to take the bait then multiple things could happen. They could install ransomware, or a monitoring

program, try and steal your credentials from your system, point your system to the internet and install more malware, send itself to all your email address book. Realistically they can do anything, the world is their oyster.

Slide (28) displays some of the techniques used by the attacker to phish you in. There are a number of ways that attackers will try and get you to click that link or open an attachment but these are the most popular signs that they are doing so:

- Do you have to do something urgently or there will be a consequence? Are your social media accounts going to be locked immediately if you don't click on the link and "verify" your account?
- Is the boss telling you to pay a bill or Microsoft telling you there is a problem with your computer? Scammers have been impersonating the World Health Organisation (WHO), the National Health Service (NHS) and other organisations to try and convince you to click on the links.
- Attackers may also try to charm you, is there something to be gained by them being so nice to you?
- Will you receive an amount of money or vouchers if you click the following link?
- Is your partner on a list of dating site leaks, do you want to see who's been checking out your Instagram page or what on earth your favourite 80s celebrity looks like now – you really won't believe it!!! People click on that link like their lives depend on it.

All of these are some of the most common attack vectors in order for you to do something you may later regret. The attacker can do anything they want once they compromise you, their next target is the system itself. So, be vigilant and question why they are contacting you.

Slides (29) to (34) are some examples of phishing emails that are real offences. Please take a short time to review these examples and see if you would fall for them? Refer to the information given above to identify why they are phishing emails.

Have you been caught out?

(35) In a lot of cases it will not immediately be obvious that something is infecting your system. It may be that any malware you've installed will lie dormant until a particular time, such as after 7pm when the attacker expects most people will be out of the office and have gone home and not notice the systems slowing down or files becoming unavailable.

In one instance that the Regional Cyber Crime Unit looked at a form of banking malware called DRIDEX was installed when an accountant was sent a spoof email, which reported to be from a colleague. When they opened the document the malware got inside the system. It then waited until

the accountant logged into the bank account and within a few minutes the company transferred £216,000 to 16 bank accounts, which was then further transferred.

Therefore, some of the most common tell-tale signs that there might be malware on your system is as follows:

- You are getting an unreasonable amount of emails – particularly from fake Anti-virus websites, same with any tech support emails saying they can fix issues for free.
- If your browser has new extensions or tools bars that you didn't/don't remember downloading.
- Excessive pop-ups are a real sign of ad-ware and other malware on the system.
- Your passwords are not working.
- Missing money from your bank account.
- Your computer is really slow and not loading the basic functions.

The solution is to update your Antivirus and run a scan. This might get rid of most of the malware, if it is not blocked by the installed malware that is. Therefore, if that is the case, it may be necessary to reboot in safe mode and go back to a restore point or if possible uninstall any suspicious new programs. Additionally, this is where you can use your backups that you've made, right? If you have backups, you can reinstall Windows and restore your files. It is also advised to change all your passwords at this point because you don't know what data has been stolen, so to be safe change them all.

If you have any suspicion that you may have been caught out – contact your IT types immediately as they can check for new software being installed, suspicious network connections being made, suspicious activity on the network from your machine etc. Contact your bank if you are missing money and report it to Action Fraud. They will give you the guidance you are looking for in the event of an attack or the aftermath.

Take 5

What is Take Five?

(36) "Take 5 is a national campaign offering straight-forward, impartial advice that helps prevent email, phone-based and online fraud – particularly where criminals impersonate trusted organisations".

So, this website, Take Five, helps you identify the criminals from the genuine people out there. They will give you helpful advice on what to do in the event of a scam and other cyber-attacks. Please take a look at their website for more advice.

In today's society, the most important data is your personal data. This is because you can be manipulated to hand over money, engage in criminal activities on behalf of the cybercriminals, and many other things these attacks want you to do. So, be cautious of what you are being asked in the first instance of contact because it may not be who you think it is.

The advice that Take Five are telling people to follow is:

- Never disclose security details, such as your PIN or password – it's never right to tell anyone these details.
- Don't assume an email request or caller is genuine – people are not always who they say they are.
- Don't be rushed – a bank or genuine organisation won't mind waiting to give you time to stop and think.
- Listen to your instincts – if something feels wrong then it is usually right to pause and question it.
- Stay in control – have the confidence to refuse unusual requests for information.

This covers phishing. The main take away from this is to always be alert and follow the advice given. It will protect you more than the person that does not. In the long run, it will save your money from those cybercriminals and no one likes to lose their hard earned money.

Working from Home

(37) Now that the government has asked everyone to work from home where they can, People need to have a heightened sense of awareness of phishing, including emails, phone calls, social media, and texts, which may be targeting them. Cybercriminals know that people will be in a more relaxed environment and they will attempt to exploit your human nature to react and the need for information. Be careful that you don't do something that could potentially harm your employer, business, company or organisation.

(38) Therefore, the majority of what has been covered above will help you survive during the time of working from home. The main take to secure your home is to:

- Change all default passwords
- Install antivirus
- Review app permissions
- Use strong passwords
- Back up your important data
- Review privacy settings for your social media accounts

- Use biometrics where possible for increased security

By following the above advice and what has been previously covered earlier in this document, will save your money, hardware, and most importantly your time. Your time is the most valuable as the investigations can go on for a very long time due to the sophistication of the attacks. This can also save you or a person a job to wipe the laptop and re-install everything before the attack.

Online Fraud

(39) Online activities, such as purchasing goods online, is safe but you should be aware that some people have alternative motives and may not send you anything in return. Before you buy anything online, make a note of the address contacting you, is it official? Does it seem legitimate? Does the company have a phone number? Is this a real number that the company uses? Check by searching for the site using a search engine. If you are unsure whether a company is trustworthy, stick with the brands that have a strong reputation. However, make sure you go to the site and not by clicking the links sent to you because there is a “50% sale” if you click this link.

(40) Always use secure sites, especially when entering any personal information like your bank details. To identify a secure site, look for the “s” in “https” at the beginning of the web address located in the URL address bar. This may also be indicated by a padlock symbol in the browser window of the address bar. This means that the website is a secure site and encrypts the traffic being sent over the internet. In simple terms this means the data is unreadable, unless you have the decryption key.

More tips for combating online safety are:

- Never give out your passwords, PIN numbers or bank account numbers – legitimate companies will never ask you for this information by email or over the phone.
- Don’t use public Wi-Fi/hotspot networks that are open to join – they might be insecure and monitored by cybercriminals.
- Use credit cards and secure payment services instead of debit cards.
- When transferring money use reliable firms with good reviews.
- Never transfer or receive money for someone else.
- Check sites’ privacy and returns policies.
- Keep a copy of your order and any acknowledgement you receive.
- Check your bank statement carefully against anything you buy online
- Keep your passwords secure
- If you’re selling online, don’t send off your product before receiving your payment.

Avon and Somerset Police
SERVE. PROTECT. RESPECT.

Next, I will help you identify and how to deal with internet fraud. You may be a victim of internet fraud if:

- There has been unusual activity or regular small amounts of money that have been withdrawn from your bank account.
- You bought an item online and it does not arrive.
- You sold something online and you don't receive payment.
- The item you receive doesn't match the original description you were given.

If you suspect that you are a victim of online fraud:

- Check with the company you dealt with to see if you can resolve the issue.
- If you have a problem with an item bought or sold using an auction site, such as eBay, check to see if they can help.
- If you paid using a credit card and the goods did not arrive, you can ask the credit card company to investigate.
- If you used an online payment service, check if you are covered by a fraud protection scheme on the service website.

If you find out that you have been a victim of fraud, please report it to Action Fraud, they can advise you on the next steps to take.

Current Common Scams

The most prevalent scams at this moment in time are to do with the Coronavirus Outbreak. These can include, personating organisations, such as the WHO. HMRC, NHS, and many others, utilising phishing emails, cold calls and text messages. Follow the guidance provided and you will be able to identify whether they are legitimate.

Other scams may be about maps or information to do with the virus spreading and data of the rate of cases, etc. don't fall for the random reach of contact. Search for the information using official sites, such as the government website, or official news sites. Don't click email attachments that run programs or take you to websites. It may show you a real website but it will also install malware on your computer at the same time.

This Action Fraud post provides some insight to the rising threat of the cyber-attacks on the UK around Coronavirus. This post also includes some protect advice.

Follow the advice given throughout this document and on slide (40) to be better prepared for an attack that may be targeting you. Preparing for an attack is the best option and much more cost-effective than being an easy target for the cybercriminals. If they think they can exploit you, they will. So, don't let them, protect yourself, your identity and your personal information.

Summary

(41) Now we have come to the end of the document and presentation. I have tried to give you as much information as I can without rambling on too much. I have covered the major topics that are currently being seen by us as a force and the other forces around the UK. Please re-read the information again when you can to remind yourself of the important actions to take, while we are house bound.

(42) Please follow the links provided and read the websites for additional information on how to protect yourself online during the pandemic. Cybercriminals are exploiting thousands of people every day and I hope this document provides you with the knowledge to protect yourselves. These are actions that only take a few minutes to activate and will save you potentially a lot of money and time in the future.

In the last few slides (43-46), there are some quick reference guides to follow, which were produced by Europol. These cover the essential protective measures mentioned above on how to make your home cyber safe. Please refer to these when needed to refresh your memory and print them off to pass on to other family/household members.

On the last slide (47) and at the beginning of this document, there are some more sources of where I got some of the information and some useful websites to look at in your own time. These sites will offer much more than what was covered in this document. I advise you to look into all the sites that are linked throughout this document in order to fully understand the reality of this situation of the ever-growing world of cyber. You can also Google the attack methods and see the severity of them in the news.

If you have any questions, please use my email address provided at the beginning. I'll be happy to reply and help in any way I can during this time of crisis. Stay Safe and be secure.