Newsletter

John Campion
Police and Crime Commissioner
West Mercia

West Mercia POLICE

The Herefordshire Hub

West Mercia Police

NOVEMBER 2020

Welcome to the November **SPECIAL EDITION** of *'The **Herefordshire Hub'*** newsletter published by the Police for the benefit of the people who live, work and visit Herefordshire. Frank, informative and full of advice; we welcome your feedback, questions or any other comments you may like to make.

At the time of writing England has locked down as Covid-19 infections increase and there is a media frenzy over an election across the Atlantic. So, following the 'prevention is better than cure' theme, I make no apologies for dominating this issue with Cyber Crime & Fraud, or more to the point, how to stay safe & avoid it.

Once again a huge thanks to those who took the time to comment so let's go straight to the question of the month:

"What are Black Friday & Cyber Monday and where did they come from?"

Both Black Friday & Cyber Monday originated in America as the beginning of pre-Christmas sales first in shops and then online. This year, Black Friday 27th November and Cyber Monday 30th November are to some degree or more just notional dates as online sales have been hitting us thick and fast already with many online stores already offering tempting bargains to get us to part with our cash.

So what follows is going to be (hopefully) full of useful advice, guidance & signposting to ensure when you part with your cash, it's because:-

- **YOU** have chosen to (and not a crook)
- **YOU** are spending it with a genuine seller
- **YOU** are safer online

.

Brambles Blog

If the mere mention of 'Cyber Security' normally sends you into a deep sleep (see left) there are a number of basic things each of us can do so that we are not the lowest hanging fruit in terms of Cyber-Crime & Fraud.

By doing these things you will not only protect yourself but others too, whether at home or in the workplace.

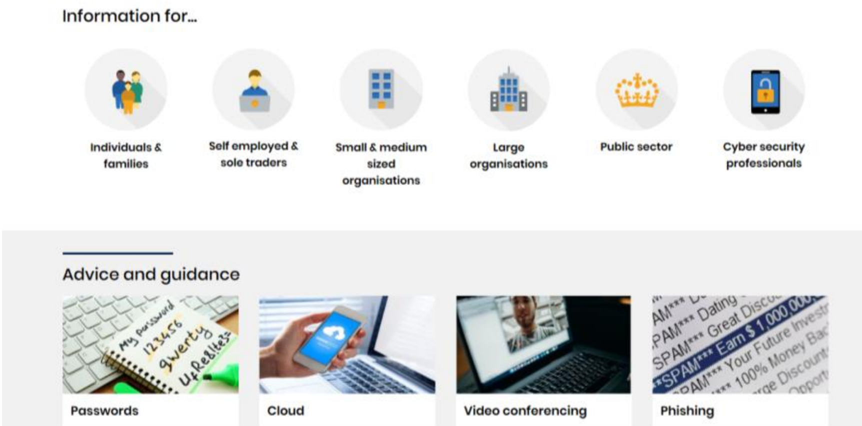
So don't be a Bramble, do read on!

National Cyber Security Centre (NCSC)

Whether at home or in business, whether you are an internet wizard, competent around a keyboard or most of it is a mystery to you, there are plenty of sources of helpful information to guide you through the maze, whatever device you are using.

The graphic on the right is from the homepage on the NCSC website and whatever category you fit into, you can see that there will be a wealth of information for you.

Here is a link that will take you straight there.
https://www.ncsc.gov.uk/



How to avoid Common Scams online, on the phone or at the door

A police officer will never call you and ask you to go to your bank and withdraw money. Fraudsters pretending to police officers are calling on the phone to get you to give them money. Don't. Hang up, wait 10 minutes and call 101 and report it.

Banks, HMRC and police will never phone you and ask you to hand over cash and will never come to the house to collect it.

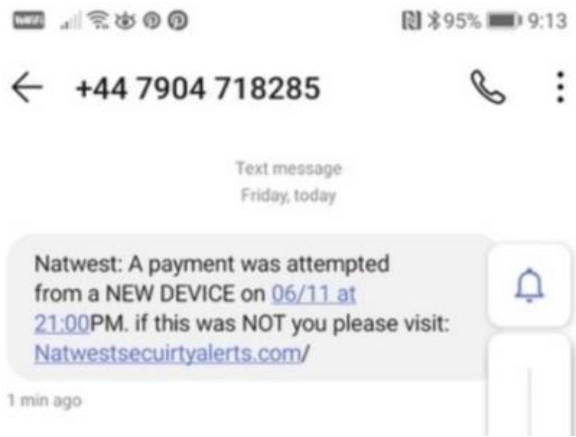
If someone comes to your door pretending to be a police officer remember that they always carry a warrant card. Ask them for it. Genuine callers will understand.

Trust your instincts: apply the same logic you would in the real world if a stranger with an unusual story asked for your money or your private information.

Can you spot a Scam Text?

Take a look at an image of a text on the right, what can you see? And what would you do?

STOP & TAKE FIVE!
https://takefive-stopfraud.org.uk/



Take five minutes to think before you respond in any way.

In this case:-

- The recipient did not bank with Natwest (oh, and Natwest tend to display their logo as NatWest – capital W)

Sometimes you only see what you expect to see

- Look at how they spell the word 'security'

It's a SCAM! You are being encouraged to click on the link Natwestsecuirtyalerts.com/ where only bad things will happen.
If you are unsure about it and have a NatWest account, log in to your account separately (NOT VIA THIS LINK) or ring a number you have obtained yourself from your own records and check that way.

Reducing the Opportunity for Crime

The Rural & Business Crime Teams can provide site specific Crime Prevention advice and guidance FREE to you at your home or place of work. They also promote Crime Reduction through presentations, talks, attending or hosting events, use of messaging systems/social media plus much more. This includes advice to protect yourself from online crime too, and that is because there are a lot of similarities between crime & fraud in your actual & online worlds.

Remember 4 Words – Urgent & Unexpected, Risk & Reward

URGENT & UNEXPECTED The Crook will try and catch you off guard, in person, online, or by phone. If you are being required to do something you didn't expect and with some urgency, then alarm bells should ring in your mind and you should STOP – THINK – VERIFY and if not 100% certain DECLINE whatever is being offered, good or bad!

RISK & REWARD Increase the RISK and reduce the REWARD for the Crook. Security marking your property for example, lowers the value of the item for the thief. Likewise adding 2 factor authentication on you devices lowers the chances for the crook to access it!

The most expensive Security measures are those that do not work for you, the best Crime Reduction measures are often simple and applied in layers, starting at your perimeter, each one making it less likely that the crook will target you. For example

Real World v Virtual World

Secure Gates = Strong Passwords

Alarm System = Firewalls Enabled

CCTV = Anti-Virus Software installed

There is no such thing as 100% secure Crime Prevention, but there is very much such a thing as Preventable Crime. Most Acquisitive crime is opportunist, where the Thief has the INTENT & CAPABILITY and all they need from you is the OPPORTUNITY.

You CAN deny them that opportunity.

RURAL MATTERS & YOUR BUSINESS MATTERS

are two campaigns operated by West Mercia Police with a focus on Rural & Business Crime.

REDUCING THE RISK

10 Golden Rules of Crime Reduction – In general, effective crime reduction is a series of layers each one designed to deter/frustrate the crook and keep them away from your property. Whilst this was written with physical property/buildings in mind, the principles apply equally well to Cyber Crime.

1. **TARGET HARDENING** – Making it more difficult for the crook to commit crime
2. **TARGET REMOVAL** – Ensuring items are out of sight

3. **REMOVE MEANS TO COMMIT CRIME** – Removing items offenders may use to commit crime
4. **REDUCE THE REWARD** – Security Marking your Property
5. **ACCESS CONTROL** – Making it time consuming and difficult for offenders
6. **SURVEILLANCE** – Ensuring offenders would be visible if they carry out a crime, using Natural (neighbours), Formal (CCTV) and Informal (Design) surveillance.
7. **ENVIRONMENTAL CHANGE** – Designing out crime by changing the environment.
8. **RULE SETTING** – Habits, closing gates, locking doors, removing keys.
9. **INCREASE THE CHANCE OF THEM BEING CAUGHT** – Layering security such as security lighting, hedge heights, concealment points, boundary protection etc
10. **DEFLECTING OFFENDERS** – Using of time switches, Alarms etc and other diversionary measures

Social Engineering

"Is the clever manipulation of the natural human tendency to trust" By this very definition it is a criminal scamming of the victim by lying or misrepresenting the situation or simply put, its Fraud or Cyber Crime.

Action Fraud

is the UK's national fraud and cybercrime reporting centre. They provide a central point of contact for information about fraud and cybercrime and list the majority of known scams with advice on how to prevent them occurring. https://www.actionfraud.police.uk/

View the website for advice Ring them on 0300 123 2040 to report.

Get Safe Online

is the UK's leading source of unbiased, factual and easy-to-understand information on online safety and I think it is a superb site for individuals and business to understand most of what you need to know about keeping yourself safe online in non-technical language. https://www.getsafeonline.org/

1980s v 2020s

Where as in the 1980s the thief may have been after your Betamax video player, (remember those?) today they are more likely to be after your data, your identity and subsequently, your cash, as they can largely act with anonymity.

Protecting your Identity with sufficient safeguards is key to thwarting a Cybercriminal.

VULNERABLE DEVICES?

Anything connected to the internet. Which today includes amongst many others, TV, Fridge Freezer, Baby Monitor, Access Control system, phone, laptop, lighting/heating controls, alarm system wi-fi enabled toaster! But my favourite….a wifi enabled curtain rail!! Yes, your curtains can open and close without you touching them ☺

You would want to know who is coming through the front door at home, do you know who is entering your virtual world via your router? Check this link outhttps://www.techradar.com/news/the-best-free-parental-control-software

CROOKS ONLINE – BY PHONE – IN PERSON

Online via fake websites, by dodgy (or phishing) emails, on the phone and in person are the typical main methods of the crook or hacker.

How to check if a website is fake https://www.getsafeonline.org/protecting-your-computer/safe-internet-use/

How to spot a dodgy email https://www.getsafeonline.org/protecting-your-computer/spam-and-scam-email/

Has your email address been hacked and/or your identity stolen?

There have always been scammers out to empty your pockets, but with the age of the internet, they've managed to get even cleverer into tricking you out of your cash. Your identity is valuable. Fraudsters know this. They can use the information you share online to pretend to be you and apply for bank accounts, mobile phones, loans or a wide range of other products or services in your name. As a victim of identity fraud, you might not realise you've been targeted until a bill arrives for something you didn't buy, or you experience problems with your credit rating, for example. To carry out this kind of fraud successfully, fraudsters usually have access to their victim's personal information, which they obtain in a variety of ways – such as through hacking and data loss, as well as using social media to put the pieces of someone's identity together. Did you know 88% of fraudulent applications for bank accounts and financial products are made online?

So, what can you do? The answer is loads! Here's a few things to be getting on with.

Close down any unused/dormant bank accounts & credit cards…….How? If you cannot remember some of them, check this Banking industry site for lost accounts http://www.mylostaccount.org.uk/aboutus.htm

Check your credit reference files this will show you what credit cards you have/have had, bank accounts etc…read the files well. You are also given a score, use that score as a check and balance, check it regularly and if your circumstances have not changed, then that score should stay roughly the same, if it plummets, and you have not changed anything, someone else probably has! You can do it so easily for a £2 statutory fee or for FREE via Martin Lewis and Money Saving Expert at https://www.moneysavingexpert.com/creditclub

Unused/dormant Social Media profiles should be deactivated and deleted…….. How? Follow the help pages on each social media platform you use, or if you have forgotten which sites you have subscribed to previously, try this from Google (remember to tick all the boxes below where you enter your name) https://www.social-searcher.com/google-social-search/

Check your email addresses & close unused /dormant accounts…….. How?

You will need to type this into your browser not click on it. https://haveibeenpwned.com/

Use strong passwords and 2 factor authentication………How?

Check this link to GetSafeOnline https://www.getsafeonline.org/protecting-your-computer/passwords/

PASSWORDS

Every good lock has a different key. Who at home has a master key for every door and window? One key to open everything?? No one does, because that one key gives access to every door/window. Lose one key, and it makes every lock vulnerable.

Treat passwords the same, and like underwear, use only once and never share!

Who has a password which is one word with a capital letter at the start and a number at the end? For example, 'Password1' – **DON'T!!** Why? Oh so easy for the Cyber Crook.

Who uses the same password for more than one device/site? – **DON'T!!** Why? If you use a password more than once, and it's compromised, then more than one device/site is vulnerable.

A password should be easy to remember and difficult to guess. The National Cyber Security Centre, Get Safe Online and loads of others give plenty of examples of what a password should consist of.

But first, have a look at the graphic below

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

OK, Brute Force to a hacker is the use of lots of computer power and some clever software to rapidly identify weak passwords.
You can see from the chart that by increasing the number of characters in your passwords, to include lower/upper case, letters & symbols it takes a whole lot longer for a password to be compromised.
So, if using on online password manager is not for you, here is a suggestion from me on what your passwords could look like.
Remember, never divulge a password to anyone….oh, and do not use the examples I give otherwise you will all have the same passwords☺

Just to add some drama to the world of passwords, as some will no doubt know, not all sites and devices use the same password formula. Some do not allow spaces, others, symbols etc…So no single suggestion will suit all, but this is as good as any. Here goes,

Think of 3 random words, 3 numbers & 3 symbols. (3 'RANDOM' words not a phrase or similar)

You are always going to use the same TWO random words, 3 numbers & 3 symbols, and the 3rd word you use will be something that reminds you of the site you are accessing, for example

Rum Gum EBAY 123!"£

Rum Gum BARCLAYS 123!"£

Rum Gum WAITROSE 123!"£

In this case, I always use (and can remember) **Rum Gum 123!"£** Think of it as your master password. The additional word would be the name of the site or something that reminds me of the name of the site I want to log on to.

Check it out for yourself using an online password checker. Try the examples given above.

https://www.my1login.com/resources/password-strength-test/

(I never put my actual password into these but I devise one that is very close)

Configuration – This is more complex but in essence for the typical domestic user this is about you understanding that each device you buy connected to the internet arrives with something called 'Admin Access'. This allows the user to do anything with device such as download, install, uninstall etc… You may wish to find out on Google how to synchronise all your devices properly, and where you have more than one user for a device, create additional profiles to restrict access to certain parts of your device. So if one of you are compromised, there is not automatic access to all your data.

Where there is more than one user on a device, you should never share the same username & password.

Firewalls – Think of these as a 'Door Security' at an event. If you have not got a ticket, you will not get in. A firewall ensures only the data you want can access your system. Some people mess with/disable them….**DON'T**. Enable them and leave alone.https://www.getsafeonline.org/protecting-your-computer/firewalls/

Anti-Virus – Using the analogy above, once inside the event, floor security will check you are complying with the conditions of entry. Anti – Virus does a similar thing, make sure you have it, it's up-to-date and enabled.https://www.getsafeonline.org/protecting-yourself/viruses-and-spyware/

Patching – Or updating. The Golden Nugget, when your operating system or any software you use tells you an update is required, do it there and then, not later/tomorrow/when you've finished, do it straight away. Why? Simply put, when a 'Patch' is issued for you to update your system/software it is **ALWAYS REPAIRING A SECURITY FLAW –** The Crooks know this and can target those devices that do not get updated.

FREE PUBLIC WIFI – Free public Wi-Fi has grown rapidly from just being available in Airport lounges and Hotels to virtually everywhere. If you have a SMART device, one that recognises where it is and connects to Wi-Fi automatically if you let it, Do you know what you are logged onto?
It is very easy for crooks to mimic locations and this sort of crime is often referred to as a ‘man in the middle attack’

How to avoid it, well if you do not need to be connected to the internet via Wi-Fi disable your Wi-Fi. With most smart phones its swipe down and press one button.
Otherwise, Turn Off Sharing, Avoid Automatically Connecting to Wi-Fi Hotspots - Use HTTPS - Use Two-Factor Authentication - Confirm the Network Name - Protect Your Passwords - Turn on Your Firewall.
You could also get a VPN – Virtual Private Network – An App you download so that when you use Wi-Fi your data is encrypted (scrambled) so the crook can’t read it.

BIG SCAMS **FRAUD ENABLERS**

SOCIAL ENGINEERING

All of the frauds described in this book come under Section 2 of the Fraud Act, Fraud by False representation. By this very definition, they involve the criminal scamming the victim by lying, or misrepresenting the situation, and this is commonly referred to as Social Engineering.

Social Engineering is defined as “The clever manipulation of the natural human tendency to trust”, and it is this natural inclination that criminals take advantage of. Usually, the criminals’ aim is to prey on people’s emotions, and get them *feeling* rather than *thinking*. This could either be a sob story, or preying on people’s greed. One of the biggest tactics they use is pressure. This could be time related “if you don’t do this in 5 minutes, you’re going to be in big trouble”, or financial “unless you agree to this, you’re going to lose thousands”. The criminal puts the victim under pressure to decide without allowing them the time to think it through.

How to protect yourself

The best defence against social engineering attacks is knowledge, once you know someone is trying to con you, the con will fail, and reading this booklet should give you that knowledge.

However, even if we’re suspicious, we’re often bad at saying “no” to people, so if you’re uncertain, you can always try these alternatives:

- “I can’t make that decision without authorisation. Let me get back to you.”
- “I will not make any decisions without speaking to someone first.”

However, don’t be afraid to simply say “no” to someone. If they’re a genuine professional, they won’t mind you taking the extra time to verify their identity or offer. If they become pushy or insistent, then odds are fairly high that it’s a form of fraud.

“An ounce of prevention is worth a pound of cure.”
Benjamin Franklin

Which leads me into a regular feature, the Rural & Business Crime Team. Paul Crumpton, John Meek & Sarah Smith work across Herefordshire as part of a larger dedicated problem solving hub. Their plea to you is:

"Please, please, please report suspicious activity, people or vehicles."

No matter how insignificant you might think it is, if it is suspicious to you, it probably is so let them know.

More and more people are contacting them directly for advice and or to relay their suspicions about someone or something.

Please keep doing so.

For a confidential conversation with Sarah, John or Paul contact them directly on:

Pc John Meek **07773 044234** **john.meek@westmercia.pnn.police.uk**
Pc Sarah Smith **07773 047243** **sarah.smith@westmercia.pnn.police.uk**
Paul Crumpton **07773 044781** **paul.crumpton@westmercia.pnn.police.uk**

You can now report non-emergency crimes on the **West Mercia Police website**

(Click on the word 'website' and it will take you straight to it – you may need to hover and press CTRL + CLICK together)

If you have any information regarding any crime you can contact police on 101, in an emergency please dial 999.

You can also contact Crime stoppers on **0800 555 111** to report any crime or criminal activity anonymously.

Well that's enough I think!

If you think a presentation on the topics (or some of them) covered above would be of use, please do let me know and we could do a virtual one via Zoom or similar if there is enough interest.

Thank you for taking the time to read this and if you have any feedback good and bad or suggestions for articles or information you would like covered please contact me on the details below.

Paul Crumpton
Rural & Business Crime Officer
Herefordshire
West Mercia Police
Mob:07773 044781
Email:**paul.crumpton@westmercia.pnn.police.uk**

Twitter: @WMPRuralMatters @WMPBusinessMatt
Facebook: look for us at Your Rural Matters and Your Business Matt

I will respond to your email as soon as possible.

If you are contacting me in relation to an emergency please call 999 or the alternative emergency number 112; for the deaf, hard of hearing or speech impaired call 18000 to use Next Generation Text Service; or use emergencySMS; or please visit our website to report crime and other matters online www.westmercia.police.uk.

On our website you can:

· Report a non-emergency incident www.westmercia.police.uk/ro/report/ocr/af/how-to-report-a-crime/

· Find about your Safer Neighbourhood Team and what's happening in your area www.westmercia.police.uk/a/your-area/

· Find advice and information www.westmercia.police.uk/advice/advice-and-information/

· Submit compliments or complaints www.westmercia.police.uk/fo/feedback/tc/thanks-and-complaints/

West Mercia
POLICE