Reducing the Opportunity for Crime

ROLE – The Rural & Business Crime Officer Provides site specific Crime Reduction advice and guidance for FREE about people, property or places at your home or at your place of work. They also promote Crime Reduction through presentations, talks, attending or hosting events, use of messaging systems/social media plus much more. For Herefordshire, please contact

Paul CRUMPTON

Rural & Business Officer (Crime Prevention) HEREFORDSHIRE

West Mercia Police

Internal 4408

External 101 then 4408

07773 044781

Paul.crumpton@westmercia.pnn.police.uk

Remember 4 Words

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.

RISK & REWARD – Increase the RISK and reduce the REWARD for the Crook. Property security marking for example, lowers the value of the item for the thief. 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. There is no such thing as 100% secure Crime Prevention, but there is 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 the two campaigns operated by West Mercia with a focus on Rural & Business Crime.

REDUCING THE RISK the 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.

Target Hardening – People, Places & Property. How secure are you? Did you know you can get FREE crime prevention advice from the police?

Target removal – Can be cost free. Is all about ensuring targets for offenders are out of sight permanently or temporarily

Removing the means to commit crime – Can be cost free. Remove any items offenders may use to commit an offence. Wheelie bins act as steps.

Reducing the pay off – Risk & Reward - Security Mark your Property.

Access Control – Control your access and you control most of what happens next. Make it time consuming and difficult for offenders

Surveillance – Ensuring offenders would be visible if they carry out a crime, using Natural (neighbours), Formal (CCTV) and Informal (Design) surveillance

Environmental change –Changing the environment to design out crime

Rule setting – Can be cost free, closing gates, locking doors, removing keys.

I**ncrease the chances of them being caught** – Layers of security take more time to overcome &increase the risk of being caught security lighting, hedge heights, concealment points etc

Deflecting offenders – use of time switches, all of the above and diversionary activities for offenders/potential offenders.

PROPERTY MARKING - 'We Don't Buy Crime' – is the title of a West Mercia Police innovative approach to reducing and disrupting the market for stolen goods and protecting homes and possessions by making them less attractive to the 'would-be criminal'. A forensic marker like SMARTWATER can be purchased online from SMARTWATER at a discounted cost of £19.95 using the checkout code of WDBCRIME25. https://shop.smartwater.com/

If a village or area (and at least 80% of residents within that area) agree to mark their possessions, West Mercia Police will provide SMARTWATER at £8.10 +Vat and place signs around the area at no extra cost. This can be further reduced by involvement of your Parish/Ward Councillors, all made possible by the Police Crime Commissioner.

Overt property marking for items in sheds/garages/outbuildings/barns etc.… again makes them less attractive to the thief, increases the risk of being caught and reduces the value when attempting to sell them on. CREMARK http://www.creproducts.co.uk/shop/default.asp is one product from many that is simple and quick to apply.

WATCH SCHEMES & CMS – I am a strong advocate of Watch Schemes. A couple of little known facts are that Neighbourhood Watch now covers any type of Watch scheme and the National Neighbourhood Watch Association as a registered charity is a separate organisation from the Police. Their website is https://www.ourwatch.org.uk/ this gives all the information needed to set up a scheme and the County volunteer administrator for NHW can help you get your scheme going. Sharing information and being informed are crucial elements of effective crime reduction. Academic research indicates Watch scheme members are 70% less likely to be victims of crime. You know your community and you will know if something or someone is unusual or suspicious**.** **Share it! Report it! Stop it!**

For the social Media users, there are some very good examples of dynamic and effective NHW schemes run on Facebook/twitter and you heard some examples of where they had prevented crime.

Community Messaging System – This is an email system managed by the Police informing you about incidents, events and advice. All you need to do is subscribe for FREE at https://www.westmercia.police.uk/cms

CONTACTING THE POLICE – In relation to the Rural & Business Crime Officer there are two Facebook sites [West Mercia Police 'Rural Matters' & West Mercia Police 'Your Business Matters] and two Twitter sites [@wmpruralmatters & @wmpbusinessmatt]

In an Emergency dial 999. In a Non- Emergency dial 101.
If you wish to speak to your local Policing team for non-emergency matters, go to the West Mercia Police website, type in your postcode or location and the contact details with a host of other information will appear. Go to https://www.westmercia.police.uk/#

If you want to report matters anonymously, contact CRIMESTOPPERS 0800 783 0137.

IS IT THE POLICE YOU NEED? 611,000 calls to West Mercia Police control room in 2017 which equates to 1+ per minute. We talked through briefly a range of advice on matters commonly referred to the Police where we have little or no powers to deal with them, or, there are other organisations better equipped to do so. Go to https://www.westmercia.police.uk/RSFT

FRAUD & SCAMS – What's the difference? – In the Banking world it matters a lot, and it directly affects you. As a guide, Fraud is something the customer has had no involvement with, for example, if a customer's card is cloned and used without their knowledge or permission, in most circumstances your money will be refunded by the bank. Whereas with a scam it's different, with a scam the customer would have provided some information or authorisation for a fraudulent payment to be made (even if they didn't realise that's what they were doing) so essentially, the bank has fulfilled the instructions of the customer. In which case there is no obligation to refund your money, however, the bank will try and recover any losses.

#becybersmart Here is a link to the West Mercia Police #becybersmart campaign with some useful basic advice for online security/safety. https://www.westmercia.police.uk/becybersmart2

Action Fraud is the UK's national fraud and cybercrime reporting center. 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/

Get Safe Online is the UK's leading source of unbiased, factual and easy-to-understand information on online safety (they say ☺) 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/

5.5M reported Fraud & Computer related crimes last year is are the single largest crime types. Whereas in the 1980's the thief may have been after your Betamax video player, 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.

CROOK v HACKER? In the 'real' world, if a burglar breaks into a premises, typically they want to steal an item of property. In the 'virtual' world the crook is likely to be after your money and the hacker might be seeking revenge, to damage your reputation or to gain respect amongst their peer group, however they both will be after your DATA.

VULNERABLE DEVICES? Anything connected to the internet. 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

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 and close down unused/dormant email accounts…….. How? Try this from the USA 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 Remember the Lock & Key board? Every lock has a different key. Who at home has a master key for every doors and windows? One key to open everything?? No one did, 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!!
Who uses the same password for more than one device/site? – DON'T!! Just like the Key analogy

above, if you use a password more than once, and its compromised, then more than one device/site is vulnerable.
A password should be easy to remember and difficult to guess, (Example of random 3 words, 3 numbers 3 symbols)

Configuration – This is more complex but in essence for the typical domestic user this is about you understanding that each device begins with 'Admin Access' that allows the user to do anything. You may wish to find out on Google how to create additional profiles to restrict access to certain parts of your device. So if you are compromised, there is not automatic access to all your data for example.
Where there is more than one user on a device, you should create separate profiles and not share the same username & password.

Firewalls – Think of these as 'Bouncer's' 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 - Turn Off Sharing - Get a VPN - Avoid Automatically Connecting to Wi-Fi Hotspots - Use HTTPS - Use Two-Factor Authentication - Confirm the Network Name - Protect Your Passwords - Turn on Your Firewall