

**December 2019**

**Tarvin and Kelsall Wards Parish Council Newsletter**

**March 2018**

**Kelsall Ward** –

**Tarvin Ward –**

**Crimes reported**

|  |
| --- |
|  |
| **Date** | **Offence** | **Details** |
| 06/12/19 | Criminal Damage | Kelsall – Damage to playground equipment. |
| 10/12/19 | Theft | Tarvin – Theft of mobile from vehicle. |
| 15/12/19 | Criminal Damage | Kelsall – Egg thrown at an address. |
| 24/12/19 | Criminal Damage | Kelsall – Plant pulled up from the garden. |
| 30/12/19 | Theft | Tarvin – Theft of medicine from a property. |
| 31/12/19 | Theft | Tarvin – Theft of a wheelie bin. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**If you see something suspicious or that you think the Police might need to know about, please report it!**

**Dial 999 in an emergency or dial 101 in a non-emergency**



Page Content

**OTHINK 5C CAMPAIGN**

​We are really pleased to be able to offer the Think5C Campaign. These are 5 simple things that people can do to keep same online.

More information on the campaign is included below. If anyone wants content for this campaign for example banner, poster or support in presenting in this topic area, please contact DC Tracey Earley on x4893 or via email.

We're living in a world where we are rapidly becoming more and more reliant on digital technology, having to adapt quickly to the many daily tasks we do. Almost nine out of 10 of us use the internet every day on either smartphones, tablets or mobiles.

We're not the only ones embracing new technology. It's not gone unnoticed by the criminal fraternity and organised crime groups, who are also adapting how they operate. Cybercrime now accounts for almost half of all recorded crime. It can affect anyone, regardless of age, gender, job or location – it's probably not a case of 'if it will happen to you' but 'when it will happen to you'.

**More than 80 per cent of known cyber attacks can be avoided by following five simple rules – we've called them the 5Cs – which will help you with your online safety and security.**

The 5Cs are:

* Create
* Cover
* Confidentiality
* Clicking
* Connection

Read on to see how each C can help improve your online safety and security.

**Create**

**Strong passwords**

There are risks to using weak passwords and for not having a separate password for your email account.

People can impersonate you to commit fraud and other crimes, including:

* Accessing your bank account
* Purchasing items online with your money
* Impersonating you on social networking and dating sites
* Sending emails in your name
* Accessing the private information held on your computer

**Here's our advice for creating a strong password:**

1. Use a strong, *separate,* password for your email account.
	* To create a strong password, simply choose three random words. Numbers, symbols and combinations of upper and lower case can be used if you feel you need to create a stronger password, or the account you are creating a password for requires more than just letters.
	* There are alternatives, with no hard and fast rules, but you could consider the following suggestions:
		+ - Choose a password with at least eight characters (more if you can, as longer passwords are harder for criminals to guess or break)
			- a combination of upper and lower case letters, numbers and keyboard symbols such as @ # $ % ^ & \* ( ) \_ +. (for example SP1D3Rm@n – a variation of spiderman, with letters, numbers, upper and lower case). However, be aware that some of these punctuation marks may be difficult to enter on foreign keyboards. Also remember that changing letters to numbers (for example E to 3 and i to 1) are techniques well-known to criminals.
			- A line of a song that other people would not associate with you.
			- Pick a phrase known to you, for example 'Tramps like us, baby we were born to run'" and take the first character from each word to get 'tlu,bwwbtr'
2. Don't use the following as passwords:
	* Your username, actual name or business name.
	* Family members' or pets' names.
	* Your or family birthdays.
	* Favourite football or F1 team or other words easy to work out with a little background knowledge.
	* The word 'password'.
	* Numerical sequences.
	* A single commonplace dictionary word, which could be cracked by common hacking programs.
	* When choosing numerical passcodes or PINs, do not use ascending or descending numbers (for example 4321 or 12345), duplicated numbers (such as 1111) or easily recognisable keypad patterns (such as 14789 or 2580).
3. Looking After Your Passwords
	* Never disclose your passwords to anyone else. If you think that someone else knows your password, change it immediately.
	* Don't enter your password when others can see what you are typing.
	* The routine changing of passwords is not recommended, unless the accounts to which they apply have been hacked, in which case they should be changed immediately. This also applies if another account or website for which you use the same login details have been hacked.
	* Use a different password for every website. If you have only one password, a criminal simply has to break it to gain access to everything.
	* Don't recycle passwords (for example password2, password3).
	* If you must write passwords down in order to remember them, encrypt them in a way that is familiar to you but makes them indecipherable by others.
	* An alternative to writing down passwords is to use an online password vault or safe. Seek recommendations, and ensure the one you choose is secure and reputable.
	* Do not send your password by email. No reputable firm will ask you to do this.

	***Using different passwords for each of your accounts can make them very difficult to remember. Consider using one of the many password vaults available on the internet, but do read reviews and get recommendations.***

**Cover**

The information held on your computer may be irreplaceable. Regularly backing up your data will ensure that you have more than one copy.

A few physical security measures can help you recover information if your computer succumbs to:

* Cybercrime.
* Hardware failure (for example, hard drive failure is a frequent occurrence).
* Accidental file deletion.
* Theft.
* Fire, flood, accidental damage.
* Catastrophic virus or spyware infections, ransomware.
* File deletion during operating system upgrades.

The data on your computer could include your documents, photos, music, video and contacts – as well as your software. Modern computer hard drives can hold massive volumes of data, making the consequences of loss through any of the above potentially disastrous. The impact could be inconvenient, stressful, time consuming and expensive.

**Keep Your Data Safe**

Backups make it simple for you to protect your data by copying and storing it somewhere other than your computer hard drive.

A variety of different methods of backing up your data are available. Whichever you choose, it is essential to observe the following:

* + Plan for total loss of your data (for example, theft of a laptop which contains all of your data).
	+ If backing up data on an external hard drive, ensure that it is stored on different premises to prevent your backup data being stolen or damaged along with your computer. If enabled by your backup device, password-protect backups to protect your privacy.

The first time data is backed up, a full backup will be carried out. Subsequent backups need only to be incremental - where only files that have been changed or added since the last backup are stored. Most modern backup processes select which mode to use automatically.

**Backup Methods**

Two principal methods of backing up your data are available. To choose which to use, you need to consider ease of use, speed, price and your own lifestyle.

**Portable Hard Drives**

An external hard disk is a fast, efficient way of backing up all of your data. Models are available that either plug into your computer's USBport, or connect via your wireless network. Most are so compact that they can easily be stored off-site.

**Online Backup (Cloud Backup)**

The use of online backup (also known as 'cloud backup') is increasingly popular owing to its added convenience, security and low cost. You may back up any data from one or two documents or photos to the entire contents of your computer, with virtually no limitation on storage space. Some providers supply limited storage free of charge, but generally the cost of backups increases proportionally to the amount of data involved.

**Confidentiality**

When talking about online safety and security, 'social engineering' means the act of manipulating or tricking people into certain actions including divulging personal or financial information … a kind of confidence trick. Social engineering exploits human nature and often plays on victims' willingness to be helpful or please others. It is a factor in many types of fraud.

Social engineering can be elaborate and is generally highly convincing, with approaches usually made by somebody you trust or in authority. It is sometimes made more believable by snippets of confidential/ personal information which the fraudsters already have about you. Private individuals and businesses can both be victims of social engineering.

**Examples of Social Engineering**

* + A fraudulent email claiming to be from your bank or credit card provider, a government department, a membership organisation or a website you buy from, telling you that you need to follow a link to supply some details – typically a password, PIN or other confidential information. This is known as *phishing*.
	+ A fraudster who has phoned you claiming to be from your bank or credit card provider, or from the police and telling you there is a problem. They ask you to confirm confidential information in order to solve the problem. This is known as *vishing*. They may even despatch a 'courier' to collect payment cards or other records from you, known as *courier fraud*.
	+ Receiving a phone call from somebody claiming to be a legitimate support agent for your computer or software, and telling you that you have a technical issue. They sound genuine, so you give them your login details which can result in fraud or identity theft. Alternatively you permit them to take over your machine remotely, resulting in them infecting it with a virus or spyware. People claiming to be from 'IT support' in your business will normally request your password in order to infiltrate company systems and data.
	+ Picking up and inserting in your computer a USB stick, memory card, CD-ROM/DVD-ROM or other storage medium that has been deliberately left for you to find, or is given to you. The device contains malware – for example virus or spyware. This is known as *baiting*.
	+ In your home or at work, inadvertently granting a criminal physical access to your computers, server or mobile device.

**How to Avoid Social Engineering Attacks**

* + Never reveal personal or financial data including usernames, passwords, PINs, or ID numbers.
	+ Be very careful that people or organisations to whom you are supplying payment card information are genuine, and then never reveal passwords. Remember that a bank or other reputable organisation will *never* ask you for your password via email or phone call.
	+ If you receive a phone call requesting confidential information, verify it is authentic by asking for a full and correct spelling of the person's name and a call back number.
	+ If you are asked by such a caller to cut off the call and phone your bank or card provider, call the number on your bank statement or other document from your bank – or on the back of your card – and not one given to you by the caller, nor the number you were called from.
	+ Do not open email attachments from unknown sources.
	+ Do not readily click on links in emails from unknown sources. Instead, roll your mouse pointer over the link to reveal its true destination, displayed in the bottom left corner of your screen. Beware if this is different from what is displayed in the text of the link from the email.

**Clicking**

Email is both an excellent communication tool and also a way that companies can inform you about their latest products and services. However, email is frequently used to deliver unwanted material which is, at best, annoying and, at worst, malicious – causing considerable harm to your computer and yourself.

The vast majority of email sent every day is unsolicited junk mail. Examples include:

* + Advertising, for example online pharmacies, pornography, dating, gambling.
	+ Get rich quick and work from home schemes.
	+ Hoax virus warnings.
	+ Hoax charity appeals.
	+ Chain emails which encourage you to forward them to multiple contacts (often to bring 'good luck').

**How spammers obtain your email address**

* + Using automated software to generate addresses.
	+ Enticing people to enter their details on fraudulent websites.
	+ Hacking into legitimate websites to gather users' details.
	+ Buying email lists from other spammers.
	+ Inviting people to click through to fraudulent websites posing as spam email cancellation services.
	+ From names/addresses in the cc line, or in the body of emails which have been forwarded and the previous participants have not been deleted.

The very act of replying to a spam email confirms to spammers that your email address exists.

**How to spot spam**

Spam emails may feature some of the following warning signs:

* + You don't know the sender.
	+ Contains misspellings (for example 'p0rn' with a zero) designed to fool spam filters.
	+ Makes an offer that seems too good to be true.
	+ The subject line and contents do not match.
	+ Contains an urgent offer end date (for example "Buy now and get 50% off").
	+ Contains a request to forward an email to multiple people, and may offer money for doing so.
	+ Contains a virus warning.
	+ Contains attachments, which could include .exe files. *A file whose name ends in ".exe" is really a program that, when opened, causes the operating system to run the program. Users who receive an .exe file as an e-mail attachment should always be sure that the file comes from a trusted source and does not contain a virus.*

	**The risks**
	+ It can contain viruses and spyware.
	+ It can be a vehicle for online fraud, such as phishing.
	+ Unwanted email can contain offensive images.
	+ Manual filtering and deleting is very time-consuming.
	+ It takes up space in your inbox.

**Email Scams**

Scams are generally delivered in the form of a spam email (but remember, not all spam emails contain scams). Scams are designed to trick you into disclosing information that will lead to defrauding you or stealing your identity.

**Examples of email scams include:**

* + emails offering financial, physical or emotional benefits which are, in reality, linked to a wide variety of frauds.
	+ These frauds include emails posing as being from 'trusted' sources such as your bank, HMRC or anywhere else that you have an online account. They ask you to click on a link and then disclose personal information.

**Phishing emails**

Phishing is a scam where criminals typically send emails to thousands of people. These emails pretend to come from banks, credit card companies, online shops and auction sites as well as other trusted organisations. They usually try to trick you into going to the site, for example to update your password to avoid your account being suspended. The embedded link in the email itself goes to a website that looks exactly like the real thing but is actually a fake, designed to trick victims into entering personal information.

The email itself can also look as if it comes from a genuine source. Fake emails sometimes display some of the following characteristics but, as fraudsters become smarter and use new technology, the emails may have none of these characteristics. They may even contain your name and address.

* + - The sender's email address may be different from the trusted organisation's website address.
		- The email may be sent from a completely different address or a free webmail address.
		- The email may not use your proper name, but a non-specific greeting such as "Dear customer".
		- A sense of urgency; for example the threat that unless you act immediately your account may be closed.
		- A prominent website link. These can be forged or seem very similar to the proper address, but even a single typed character's difference means a different website.
		- A request for personal information such as username, password or bank details.
		- You weren't expecting to get an email from the organisation that appears to have sent it.
		- The entire text of the email may be contained within an image rather than the usual text format. The image contains an embedded link to a bogus site

**Use email safely**

* + Do not open emails which you suspect as being scams.
	+ Do not forward emails which you suspect as being scams.
	+ Do not open attachments from unknown sources.
	+ **If in doubt, contact the person or organisation the email claims to have been sent by ... better safe than sorry.**
	+ Do not readily click on links in emails from unknown sources. Instead, roll your mouse pointer over the link to reveal its true destination, displayed in the bottom left corner of your screen. Beware if this is different from what is displayed in the text of the link from the email.
	+ Do not respond to emails from unknown sources.
	+ Do not make purchases or charity donations in response to spam email.
	+ Don't click on 'remove' or reply to unwanted email.
	+ Check junk mail folders regularly in case a legitimate email gets through by mistake.

**Connection**

Wireless networks have revolutionised the way we can use computers and mobile devices, both in the home and office – and when we are out and about. Home and office wireless networks make it easier to use the internet and send and receive email in any room in the building and even outside... and enable visitors to do likewise. 'Public' wireless networks or hotspots mean that we can do the same in places like cafés, hotels and pubs. And plug-in mobile broadband devices, or 'dongles,' provide even more flexibility, allowing you to work online where there is cellular 3G or 4G coverage.

Home/office/mobile and public WiFi (as wireless connections are commonly known), There are some common potential issues, whilst each has its own particular risks. You can protect yourself easily with a few simple precautions.

**Home/Office Wireless Networks**

**The Risks**

If your wireless hub/router/dongle is not secured, other people can easily gain access to it if they are within range. This can result in unauthorised people doing the following:

* + Taking up your bandwidth – affecting the online speed of your own computers and other devices.
	+ Using your download allowance, for which you have paid your Internet Service Provider (ISP).
	+ Downloading inappropriate material, which would be traced to your address and not their computer.
	+ Accessing sensitive information that you may be sending or receiving online.

**Safe Wireless Networking**

All of the above risks can be avoided simply by ensuring that the wireless hub/router/dongle that you wish to connect to, is secured. To check that this is the case, simply search for available wireless networks, and those that are secured will be indicated with a padlock symbol.

When you first connect a computer, smartphone, tablet, printer or any other wireless-enabled device to any wireless hub/router/dongle, you will be prompted to enter a password/key, provided the network is in secure mode. This will enable the device to connect on this occasion and normally, for future use. The Wi-Fi key and admin password will be supplied with the hub/router/dongle, but we recommend you change it to secure ones of your own choice.

Keep Wi-Fi codes safe so that others cannot access or use them.

Remember that the access code is usually printed on the hub/router, so take care to either remove it, or make the hub/router itself inaccessible in the event of an intrusion or people you do not know on your property.

**Public WiFi**

**The Risks**

The security risk associated with using public WiFi is that unauthorised people can intercept anything you are doing online. This could include capturing your passwords and reading private emails. This can happen if the connection between your device and the WiFi is not encrypted, or if someone creates a spoof hotspot which fools you into thinking that it is the legitimate one.

Alternatively, you may simply be prompted to log in to enable internet access. This will tell the operator that you are online in their café, hotel or pub. There is almost certainly no security through encryption.

**Safe Public WiFi**

* + Unless you are using a secure web page, do not send or receive private information when using public WiFi.
	+ Wherever possible, use well-known, commercial hotspot providers such as BT OpenZone or T-Mobile.
	+ Businesspeople wishing to access their corporate network should use a secure, encrypted Virtual Private Network (VPN).
	+ Ensure you have effective and updated antivirus/antispyware software and firewall running before you use public WiFi.

**Other Advice**

* + Don't leave your computer, smartphone or tablet unattended.
	+ Be aware of who is around you and may be watching what you are doing.

Bottom of Form

**UTBUILDING SECURITY**

**Surgeries and Meetings in January**

**Delamere Community Centre- Sunday 19th January 1000-1100hrs**

**Tarvin Community Centre- Friday 3rd January – 1800-1900hrs**

**Thursday 9th January 1300-1400hrs**

**Saturday 18th January 1000-1100hrs**

**Thursday 23rd January 1800-1900hrs**

**Thursday 30th January 1000-1100hrs**

**Kelsall Community Centre- Saturday 4th January -1800-1900hrs**

**Friday 10th January 1300-1400hrs**

**Saturday 18th January 1200-1300hrs**

**Saturday 25th January 1800-1900hrs**

**Thursday 30th January 1200-1300hrs**

**Keeping In Touch**

|  |
| --- |
| **Local Officer Contact Details – PCSO 22206 Sue Keers****Police community support officer****Tel - 101****Email –** **sue.keers@cheshire.pnn.police.uk**  |
| User PhotoUser Photo |

**Local Officer Contact Details – PC 3862 Rob Boulton**

**Beat Manager**

**Tel - 101**

**Email – robert.boulton@cheshire.pnn.police .uk**