The SKYLARK

Longstowe Parish Newsletter

July 2017

Village News

Village Hall – Well, we are sure the drums have been sounding as to how well the renovation of the village hall is going! As you will hopefully agree, it's starting to look wonderful. The cladding is 75% done and there will now be a slight hold on the work to allow for the windows on the front of the façade to be fitted, before our builders, Creative Builders and Interior Ltd, put the final wall of cladding.

Inside the Hall, 90% of the work has been completed and we now have freshly painted walls and ceilings, and a fab new floor. We decided to spend a little extra money on the server hatch, replacing the current guillotine system, with a pair of hinged double doors. These are not yet fitted, but should be with us for later cricket fixtures, and the Fete. There will also be a stable door made to the bar, so that drinks can be served to the outside without the need for muddy boots coming through the main hall.

We have lots of other things we want to do in terms of cloakrooms, disabled toilets facilities etc. but for this we still need to fundraise. Therefore, please do support The village Fete, and look out for details of the forthcoming Beer Festival that is currently being planned.

The Longstowe Village Hall Committee

Village fete – *September 17th*

The Village fete this year is scheduled for the 17th of September and its set to be a scorcher! (Obviously this is unconfirmed) so put the date in your diaries!

It has been suggested that a little light activity might make for a fun event and we are floating the idea of a fundraiser cricket match and tea. The idea would be to gather enough people for 4 teams, with a small entry fee (a few pounds). All men/woman and children would be welcome to play for a fun game and those not playing could support the event by trying to pick the winning team!
Email clare.rebbeck@cruk.cam.ac.uk or call 269 041 if you would like to be involved. Any money raised from events such as this would go towards the village fund.

The Longstowe Show however will not be held this year. This decision is based on poorly supported shows over the last two years.
We have seen the level of entries, over the past ten years drop from enough to fill the main hall, to the point where there was barely enough material to fill one table in the corner of the hall. The village hall committee regrets having to make this decision but as things stand there seems little point in pursuing this no longer adequately supported event. The committee does not rule out any possibility of resurrecting The Show in future years, it all depends on YOU supporting it and making your opinion heard!

In due course, The Hollis Cup will be used for another suitable event though as yet no decision has been made. Your comments are welcomed, please either email mrpeterwhite@btinternet.com or telephone 01954 719669 and your comments will be passed on to The Village Hall Committee.

Peter White (VH Committee member)

Longstowe Parish Council meetings are usually held on the third Thursday of each month (except August) at 7.15pm in the Village Hall. Everyone is welcome.

July 20th
September 21st
October 19th
November 16th
December 21st

The Agenda and Minutes for each meeting are on the website at http://www.scambs.gov.uk/content/longstowe.

Neighbourhood Watch

Your co-ordinators are:

Deborah Hemmins 719638
Peter Hemmins 719372

If you see an incident, please take all the details and jot them down. Numbers, dates, times, descriptions. If matters are so urgent then dial 999 directly. Otherwise telephone 01345 456 4564.
Website: www.cambs.police.uk

Locally Wanted / Available / recommended

(If you would like to add to this feature please email The Editor)

Wanted: Looking for an old-fashioned wooden kitchen table (almost) any condition.
Peter. 719669
mrpeterwhite@btinternet.com

Recmmended: We can recommend Cambridge Asbestos Removal Ltd if you need any work done – they did a quick and clean job for us.
Bobbie Coe.

Bourn to Run!

Get your running shoes on and raise money for the Bourn Primary Academy.

The following messages have been sent on behalf of Action Fraud (National Fraud Intelligence Bureau)

If you have been a victim of fraud or cyber crime, please report it to Action Fraud at http://www.actionfraud.police.uk/ or alternatively by calling 0300 123 2040

Anyone with any information should call the police on **101** or Crimestoppers, anonymously, on 0800 555111

How to protect yourself

Having up-to-date virus protection is essential; however it will not always prevent your device(s) from becoming infected.

- **Never divulge passwords or pin numbers.**
- Always check the validity of any text message from your credit card provider by contacting them through the number provided at the back of the card or on the credit card/bank statement.
- Beware of cold calls purporting to be from banks and/or credit card providers.
- If the phone call from the bank seems suspicious, hang up the phone and either wait for 10 minutes before calling the bank back or use a different phone. Again, refer to the number at the back of the card or on the bank statement in order to contact your bank.
- Always be wary of unsolicited calls. If you're unsure of a caller's identity, hang up.
- Don't call numbers from pop-up messages on your computer.
- Never allow remote access to your computer.
- Microsoft or someone on their behalf will never call you.
- Always install software updates as soon as they become available. Whether you are updating the operating system or an application, the update will often include fixes for critical security vulnerabilities.
- Install anti-virus software on all devices and keep it updated.
- Create regular backups of your important files to a device (such as an external hard drive or memory stick) that isn't left connected to your computer as any malware infection could spread to that too.
- Only install apps from official app stores, such as Google's Play Store, or Apple's App Store as they offer better levels of protection than some 3rd party stores. Jailbreaking, rooting, or disabling any of the default security features of your device will make it more susceptible to malware infections.
- An email address can be spoofed. Don't open attachments or click on the links within any unsolicited emails you receive, and never respond to emails that ask for your personal or financial details.
- Do not enable macros in downloads; enabling macros will allow Trojan/malware to be installed onto your device.
- The sender's name and number in a text message can be spoofed, so even if the message appears to be from an organisation you know of, you should still exercise caution, particularly if the texts are asking you to click on a link or call a number.
- Don't disclose your personal or financial details during a cold call, and remember that the police and banks will never ring you and ask you to verify your PIN, withdraw your cash, or transfer your money to another "safe" account.
- If an individual claims to be a police

officer ask for their name and rank, force, and examine any identification presented; this is always good practice but especially important if they are not wearing a uniform.
- The Police will never ask for your passwords or PIN details. Do not give this information to anyone.
- The Police will never request that you withdraw/transfer any money to them or to a 'safe' account.
- If you think your bank details have been compromised, you should contact your bank **immediately**.

For further information on any of the following, please contact the Clerk at LongstowePC.Clerk@hotmail.com

Smishing – the term used for SMS phishing – is an activity which enables criminals to steal victims' money or identity, or both, as a result of a response to a text message. Smishing uses your mobile phone (either a smartphone or traditional non-internet connected handset) to manipulate innocent people into taking various actions which can lead to being defrauded.

Tech-Support scammers claiming to be from Microsoft who are taking advantage of the global WannaCry ransomware attack.
One victim fell for the scam after calling a 'help' number advertised on a pop up window. The window, which wouldn't close, said the victim had been affected by WannaCry Ransomware. The victim granted the fraudsters remote access to their PC after being convinced there wasn't sufficient anti-virus protection. The fraudsters then installed Windows Malicious Software Removal Tool, which is actually free, and took £320 as payment.
It is important to remember that Microsoft's error and warning messages on your PC will never include a phone number. Additionally Microsoft will never proactively reach out to you to provide unsolicited PC or technical support. Any communication they have with you must be initiated by you.

Distraction Burglaries
Police are urging residents to be vigilant and to look out for elderly relatives and neighbours following a spate of distraction burglaries in Cambridge City and South Cambridgeshire. Most of the burglaries have involved criminals claiming to be either police officers or Neighbourhood Watch members or waterboard officials. Water company employees will try whenever possible to make an appointment before visiting a home.
Be especially wary of anyone saying that they are from 'the water board' as the water board does not exist. A genuine water company employee will name the water provider, such as Cambridge Water or Anglian Water, and will carry a company identification card.

Not Sure Don't Open the door
Before opening the door to any stranger, stop.
LOCK – Are your back windows and

doors locked? If not, lock them before you answer the front door as distraction burglars often work in pairs - one distracts, while the other steals

STOP - Are you expecting anybody? Ask the caller: What are you here for? Can I check your I.D.? Do you have paperwork relating to your call?

CHAIN - Put this on before you open the door. If you have not got one, it is a worthwhile investment. It will give you that extra 'safe space' and barrier between you and the caller and then,

CHECK - Ask for their identification card, take it and look at it carefully. Close the door and check the number in the phone book - not the number on the card. If they are genuine they will not mind waiting or coming back another day.

Not sure? Don't open the door!

TIP Security devices such as door-chains and bars will give you more time to think; and can deter bogus callers from entering your home.

- Look out for phrases such as **'I'm from the waterboard'** this should ring alarm bells straight away. Which company?
- Many organisations have password schemes (gas/ utility companies) and free phone hot lines to check the identity of their staff.
- If you are still not sure if the caller is genuine – contact the police on **999** straight away.
- Do not keep large amounts of cash at home, use a bank or local Post Office.

Ransomware

Following the ransomware cyber attack on Friday 12 May which affected the NHS and is believed to have affected other organisations globally, Action Fraud has issued an alert urging both individuals and businesses to follow protection advice immediately and in the coming days. Ransomware is a form of malicious software (Malware) that enables cyber criminals to remotely lock down files on your computer or mobile device. Criminals will use ransomware to extort money from you (a ransom), before they restore access to your files. There are many ways that ransomware can infect your device, whether it be a link to a malicious website in an unsolicited email, or through a security vulnerability in a piece of software you use.

We urge people to be cautious if they receive any unsolicited communications from the NHS.

Key Protect messages for **businesses:**

https://www.ncsc.gov.uk/guidance/ransomware-latest-ncsc-guidance.

For additional in-depth technical guidance on how to protect your organisation from ransomware, details can be found here: https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

Phishing emails

Fraudsters are sending out a high volume of phishing emails to personal and business email addresses,

pretending to come from various email addresses, which have been compromised.

The subject line contains the recipient's name, and the main body of text is as below:

"Hi, [name]!

I am disturbing you for a very serious reason. Although we are not familiar, but I have significant amount of individual info concerning you. The thing is that, most likely mistakenly, the data of your account has been emailed to me.

For instance, your address is:

[real home address]

I am a law-abiding citizen, so I decided that personal data may have been hacked. I attached the file – [surname].dot that I received, that you could explore what info has become obtainable for scammers. File password is – 2811

Best Wishes,"

The emails include an attachment – a '.dot' file usually titled with the recipient's name. This attachment is thought to contain the Banking Trojan Ursniff/Gozi, hidden within an image in the document. The Ursniff Banking Trojan attempts to obtain sensitive data from victims, such as banking credentials and passwords. The data is subsequently used by criminals for monetary gain.

And remember, if something appears too good to be true, it probably is!

Tourists Targeted By Fake Police Officers

There has been a series of recent incidents reported to Action Fraud where a lone fraudster has approached victims whom they believe to be unfamiliar with the local area. They make an excuse to talk to the victims such as enquiring about directions or offering a recommendation for a good hotel.

After this interaction, several other fraudsters will intervene purporting to be police officers in plain clothes and will sometimes present false identification as proof. The fake officers will then give a reason to examine the victims' wallet, purse or personal items. They may also examine the first fraudster's items or try to tell victims that the first fraudster is suspicious in order to gain victim trust and appear more realistic in their guise.

After all the fake police 'checks' are finished, victims have then reported being handed back their personal items only to later realise that a quantity of money or valuables were missing.

LONGSTOWE FETE
and
VILLAGE SHOW

SUNDAY 17th September 2.00pm

BAR - BBQ - Teas
Stalls - Raffle
and
*** ENTERTAINMENTS ***

PLEASE deliver donations by
Thursday 14th Sept

to one of the following, or contact and we will collect:
Peter White (80 Old N Rd, 719669) or **Jane Bowden (Glebe House, 719737)**

BOTTLES
TOYS - BOOKS - RAFFLE PRIZES
BRIC-A-BRAC (no clothes, thank you) - PLANTS
CAKES - HOME PRODUCE (can also be delivered to Village Hall on the day)

Please send items for the next edition
By the 15th September

Clare.rebbeck@cruk.cam.ac.uk