September Cyber Scam Update

Butlin's Data Breach

Butlin's has admitted that it has suffered a data breach that may have exposed details of 34,000 guests. Personal information contained within the records accessed by hackers includes names, booking reference numbers, arrival dates, home addresses, email addresses, and telephone numbers.

TOP TIPS

- Be aware of any correspondence, whether via email or on the phone, relating to a Butlin's booking you may have made - especially if this asks you to share your personal details or financial information
- Monitor any unexpected transactions in your bank account, just in case any financial details have been shared
- Check that changes have not been made to your booking without your authorisation

Pension Scams Action Fraud

The Financial Conduct Authority (FCA) and The Pensions Regulator (TPR) are urging the public to be vigilant when receiving unsolicited offers about their pensions and to check who they are dealing with. This comes after figures show that a total of 253 victims reported to Action Fraud that they had lost more than £23 million to pension scammers in 2017, which equates to an average loss of £91,000 per victim.

TOP TIPS

- Reject unexpected pension offers whether made online, on social media or over the phone.
- Check who you're dealing with before changing your pension arrangements – **check the FCA Register** or call the FCA contact centre on 0800 111 6768 to see if the firm you are dealing with is authorised by the FCA.
- Don't be rushed or pressured into making any decision about your pension.
- Consider getting impartial information and advice.

Cyber Crime Unit Scam Call

We have been made aware of a scam call to Warwickshire residents, claiming to be from the 'Cyber Crime Unit'. Residents have reported to us that the scammers claimed that the homeowner's internet line was compromised and would be turned off, unless their instructions were followed.

With these types of calls, the cold callers are typically after one of two outcomes: seeking to gain remote access to your computers or they will fix the (non-existent) problem, and state there is a charge for the 'service' they have provided, which they pressure you into paying.

TOP TIPS

- Trust your instincts. If something doesn't seem right about a phone call, email or other message, then hang up the phone, or delete the message- Don't give any personal information
- Do not allow remote access to any of your devices

If You Are Affected

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or http://www.actionfraud.police.uk

If you would like support as a result of becoming a victim of any crime, contact Victim Support on 01926 682 693.

September Cyber Scam Update

Superdrug Data Breach

Superdrug has become the latest big-name high street brand to have suffered a breach of customer data, after hackers apparently tried to hold the firm to ransom. The retailer has been sending emails out to those affected after reports suggested hackers contacted the firm to say they had data on 20,000 customers.

TOP TIPS

- Change the password for your Superdrug account - and any else with the same, or highly similar, passwords
- If Superdrug have emailed you, log into your accounts via the Superdrug website, rather than clicking on an email link - scammers may still pretend to be the company, and send out scam emails to capture more information about you
- Be aware of any scam phone calls or text messages, as phone numbers are known to have been breached

Follow Us on Social Media for the Latest Cyber Crime News

Facebook facebook.com/cybersafewarwickshire
Twitter @CyberSafeWarks
Instagram Cyber_Safe_Warks
or visit www.cybersafewarwickshire.com

Gift Card Fraud

Action Fraud is warning the public to 'Stay Tuned to Fraud' as fraudsters are contacting victims, claiming to be from well-known organisations including Her Majesty's Revenue and Customs (HMRC). Fraudsters are using online store gift cards to collect money from victims because they can be easily redeemed and sold on. The fraudsters don't need the physical card to redeem the value and will instead use tactics to persuade victims to purchase gift cards in large amounts and read out the serial code on the back over the phone.

TOP TIPS

- No genuine organisation will ask you to pay taxes, bills or fees using iTunes Gift Cards, or any other type of voucher.

MONTHS TOP TIP Shopping Scams:

Protect yourself from Shopping Scams:

- Use trusted websites, with HTTPS and the padlock within the address bar.

- Be aware of scam emails, text messages and social media posts offering must have items for low prices.
- Be aware of phishing emails appearing to come from payment sites/auction sites stating your account has been suspended.

DVLA Issue Scam Warning

DVLA is reminding customers that the only official place to find our services and information is on GOV.UK. Scam Emails and text messages might ask up to update personal details or that you are due a refund. There might also be fake websites that try to pass themselves off as the DVLA.

TOP TIPS

- Only use GOV.UK so you can be sure that you're dealing directly with DVLA.
- The DVLA won't send messages asking you to update your personal or payment details.

If You Are Affected

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or http://www.actionfraud.police.uk

If you would like support as a result of becoming a victim of any crime, contact Victim Support on 01926 682 693.