DORSET POLICE CYBER CRIME UNIT

CYBER CRIME PREVENTION TOOLKIT

A collection of recommended resources to help improve cyber awareness and cyber readiness for individuals and organisations.

CYBER CRIME AFFECTS US ALL

Between April 2018 and March 2019, in Dorset alone, £16.5m was lost to fraud. Across the UK, victims lost a total of £2.2bn.

Phishing emails, scam phone calls, and malware are just a few of the ways we can be targeted online, and the threat evolves every day. That's why it's so important that we know what to look out for, and how to defend ourselves.

In this document, you'll find some of the top resources available to bolster your cyber defences, and help keep you safe online.

FIND US ONLINE

www.dorset.police.uk/cybercrime

Facebook - @DorsetPoliceCyberCrime

Twitter - @DP_CyberCrime

LITTLE BOOK OF CYBER SCAMS

Aimed mainly at businesses, the Little Book of Cyber Scams contains some great tips to help protect your data. Get your free copy by scanning this QR code.

WWW.DORSET.POLICE.UK/CYBERCRIME

Dorset Police Cyber Crime Units home page contains useful information, and links to resources to help keep you safe online. For further advice, our Cyber Protect Officer, Chris Conroy, can be emailed at **cybercrimeprevention@dorset.pnn.police.uk**.

WWW.NCSC.GOV.UK

The NCSC is part of GCHQ, the government's intelligence and security organisation. As such, they are very well placed to provide impartial cyber security guidance. On the NCSC website, you'll find cyber advice for individuals and families, self-employed and sole traders, small to medium businesses, large organisations, public sector bodies and cyber security professionals.

WWW.ACTIONFRAUD.POLICE.UK

Action Fraud is the UK's national reporting centre for fraud and cyber crime, covering England, Wales and Northern Ireland. Should you fall victim, you should report to Action Fraud by visiting their website, or calling 0300 123 2040. The website also features warnings about emerging scams, helping to keep you one step ahead.

WWW.TAKEFIVE-STOPFRAUD.ORG.UK

Take Five is a campaign funded by UK Finance and Government to help consumers protect themselves from financial fraud. It offers plenty of advice on a number of known scams, as well as a quick test to see how scam aware you really are.

WWW.FCA.ORG.UK/SCAMSMART

The Financial Conduct Authorities ScamSmart site can help you determine whether or not an investment or pension opportunity is genuine, or if it's best avoided.

WWW.HAVEIBEENPWNED.COM

Have I Been Pwned allows you to search across multiple data breaches to see if your personal details have been compromised. It can determine whether your email address and password are exposed online and provides guidance on how to secure your accounts if they are.

TOP TIPS FOR CYBER SAFETY

1. **Use strong, complex passwords.** Pets names, dates of birth and football teams don't make for good passwords. Use a combination of upper and lower case letters, numbers and special characters. A passphrase, made up of three random words, is a good base to start with.

2. **Install a reputable antivirus package.** Antivirus programs are a safety net, protecting you against any malicious files that find their way on to your devices. Make sure its always on, and always up to date.

3. **Install updates.** Make sure you install software updates as soon possible. They often contain important security fixes

4. **Be careful where you click.** Take care with links and attachments in email. If it's unexpected, or suspicious, don't click. Double check the address of the website the link takes you to (by hovering your mouse over the link). Criminals often take advantage of spelling mistakes to direct you to a malicious site.

5. **Beware of public Wi-Fi.** Whilst it's absolutely fine for casual browsing, free Wi-Fi is not secure. Sensitive data, like passwords or banking details, can be spied upon. Use your mobile data, or a Virtual Private Network (VPN) instead.

6. **Back it up.** Make a second or third copy of everything you care about. If you suffer from a ransomware attack, restoring files from a removable hard drive is much easier, cheaper, and more reliable than paying a criminal for your files back.

7. **Be careful what you share.** Where you go to school, or work, or on holiday… this information is more valuable than some people think. Information shared on social media can be used by scammers to impersonate potential victims, or guess password reset questions, for example.

8. **Keep your devices safe.** Use passwords, pin codes or biometrics where available.

WWW.TURNON2FA.COM

Two Factor Authentication is an additional layer of protection on top of your password. It can significantly reduce the risk of your online accounts being compromised. 'Turn On 2FA' provides step by step guides for activating Two Factor Authentication on a number of major sites, including Facebook, Twitter, Gmail and Amazon.

WWW.PHISHINGQUIZ.WITHGOOGLE.COM

Developed by Jigsaw (a Google subsidiary), this free phishing quiz lets you explore a number of sample emails and make a judgement as to whether it's legitimate, or a phishing email. It provides helpful tips to spot fraudulent emails, should any slip through the net.

FOR BUSINESSES:

WWW.CYBERESSENTIALS.NCSC.GOV.UK

Cyber Essentials helps you to guard against the most common cyber threats and demonstrates your commitment to cyber security. It is an accreditation scheme that reassures clients and suppliers that you are working to secure your infrastructure against cyber-attacks, and can attract business with the promise you have cyber security measures in place. Accreditation is a minimum requirement for a number of government contracts. However, if your organisation does not aspire to this, the site still provides some useful guidance, explained in simple, non-technical terms.

WWW.NCSC.GOV.UK/SECTION/KEEP-UP-TO-DATE/CISP

The Cyber Security Information Sharing Partnership (CiSP) is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential environment. It aims to increase cyber awareness, and reduce the impact of cyber crime on UK businesses. CiSP provides an early warning of cyber threats, and the ability to learn from the experiences, mistakes and successes of other users.

To find out more, and to register, visit the website. If you have any specific queries about CiSP, please email cisp@ncsc.gov.uk.

MAKE USE OF THE FREE RESOURCES AVAILABLE FROM THE NCSC

The National Cyber Security Centre have a whole range of useful cyber security guides, providing simple, non-technical guidance to help improve your organisations cyber security.

Take the time to look at their e-learning package 'Stay Safe Online: Top Tips For Staff', which can be completed online, or downloaded and added to your own e-learning ecosystem.

The training covers phishing, strong passwords, device security and incident reporting, and is available completely free of charge.