CYBER CRIME NEWS

ISSUE 6 • SEPTEMBER 2023

WELCOME TO CYBER CRIME NEWS

Welcome to the September issue of Cyber Crime News – the bi-monthly newsletter from Dorset Police to keep you up to date with the latest news, campaigns, crime prevention guidance and support for businesses. Please share with your networks.

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

PRODUCED BY DORSET OPCC AND DORSET POLICE

DORSET POLICE

RANSOMWARE ATTACKS

In last month's issue we discussed the recent surge in ransomware attacks, with a number of local organisations being impacted by new and emerging strains.

New strains of ransomware appear on a regular basis, and those that are already in use are frequently updated to remain effective. However, criminal groups generally rely on tried and tested methods to compromise their victims.

These include, but are not limited to, social engineering, phishing, malicious attachments and – as seems to be the case in the majority of recent local reports – misconfigurations.

Since the pandemic, workplaces have become more dynamic. Hybrid working means that many of use work at both the office and our homes and as such, remote desktop tools have become more prominent. These allow us to interact with our work network as if we were sat in the office, from the comfort of our own homes.

However, if not managed properly, they can also provide a gateway into our organisations for people we would rather keep out.

Typically, accessing a network through a remote desktop requires a user to log in – the credentials required may vary from tool to tool, but generally users will need to provide an email address and a password. This, of course, is an inherent weak point – this defence relies on users implementing strong passwords and, crucially, keeping them secret.

This is easier said than done in a world where social engineering is becoming increasingly effective, and phishing emails are increasingly realistic.

Malicious phone calls and emails or – as was the case in the last issues example – spoofed log in portals can easily catch people out. This is especially true when users are perhaps facing pressure to complete a task, for example.

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

PRODUCED BY DORSET OPCC AND DORSET POLICE

DORSET POLICE

SO, WHAT CAN WE DO TO PROTECT OURSELVES?

There are a few measures organisations can put in place to keep their remote desktop connections secure. These include:

1. Multi Factor Authentication (MFA) – MFA requires additional information before a login attempt is approved. This information is usually a code, which can be sent by SMS or generated within an authenticator app. It is generally accepted that authenticator apps are more secure than SMS based MFA. Implementing MFA provides a barrier to anyone who successfully obtains login credentials, preventing criminals from putting them to use.
2. Sign in risk assessment tools – If your remote desktop solution allows it, make use of these tools to check things like geographic location, or device compliance. If things like location, IP address or device details do not meet the criteria, access can be blocked.
3. Limit the damage of a successful breach – remote desktop connections can be configured to grant access to selected resources only, based on a persons role. This can help limit access to more sensitive material within your network. Connections can also be configured so that files cannot be transferred from the virtual device to the offenders physical device, reducing their ability to extract data.

This is by no means an exhaustive list of the measures we can implement, and further advice can be sought from the National Cyber Security Centre. You can find more about their recommended technical controls here - **Action 5 - Put technical controls in place - NCSC.GOV.UK**

Banking scams are, unfortunately, commonplace nowadays. Whilst there are many ways in which they can be carried out, the more frequently seen banking scams involve the scammer making a phone call and claiming to be from the victim's bank.

Catching people off guard, or perhaps reaching someone in some way vulnerable, scammers know just what to say in order to trick people in to handing over their hard-earned money.

A Dorset resident was recently contacted by a scammer who claimed to work for a high street bank. They stated that the victims online bank had been compromised, and they needed to guide them through the process of setting up a new one. Through the use of various social engineering techniques, the scammers convinced the victim to hand over their life savings – just over £90,000.

This technique has been widely used against members of the public for a long time, but in recent months Action Fraud have recorded an increase in cases where businesses have been successfully exploited.

SINCE JUNE 2023, 31 BUSINESSES ACROSS THE COUNTRY HAVE REPORTED FALLING VICTIM TO THIS SCAM, WITH REPORTED LOSSES TOTALLING OVER £3.8M.

Whilst there is no set script for a scam like this, scammers generally use the following format:

1. The victim is contacted by someone claiming to represent their bank, or a financial services vendor. They will convince the victim to install remote access software, claiming it is required to perform an important update.
2. The victim is then instructed to log in to their online banking account. At this point, the scammers will give a reason for needing to blur the screen. This, of course, masks what they are doing – making fraudulent transactions.
3. The scammers may ask the victim to read out a series of numbers they claim to have sent to the victims mobile. This is actually the one time verification code from the victims bank, which essentially authenticates the scammers transaction.

Whilst many businesses will have measures in place, such as dual signature / authorisation processes, others may not. As such, it is worth remembering the following:

1. Banks will never ask for remote access to your computer or smartphone. You should never install software as a result of an unsolicited call, browser pop-up or text message.
2. One time verifications codes are sent by the bank directly to you, and should not be shared – not even with bank employees.
3. Take the time to verify any contact from someone who claims to be from your bank. If the call is suspicious, or unsolicited, hang up. Then, after waiting a few minutes for the line to clear, call your bank using the contact details on your credit or debit card, paper bank statement, or bank website.
4. If you are concerned that your device may be infected with malware, or something else that could grant criminals access, have a look at the advice from the National Cyber Security Centre on recovering infected devices – **https://www.ncsc.gov.uk/guidance/hacked-device-action-to-take**

CONTACT US FOR FREE CYBER AWARENESS TRAINING FOR BUSINESSES

Dorset Police offer free and impartial cyber awareness sessions to businesses of all sizes – from a handful of staff to hundreds.

The sessions provide organisations with National Cyber Security Centre backed advice and guidance, covering cyber security fundamentals, including how to spot and respond to various cyber threats.

Sessions can be delivered either in person, at a time and location that suits your needs, or virtually, via your chosen video conferencing platform.

If your business has a specific cyber security concern or you just don't know where to start, we can tailor presentations to ensure your needs are met.

If you feel this would be of benefit to your company, please get in touch – we can then discuss your needs, and book in a cyber awareness training session at no cost to you.

To arrange a cyber awareness session, email us at: cybercrimeprevention@dorset.pnn.police.uk

ADDITIONAL HELPFUL ADVICE

Ransomware protection can be a technical area to negotiate, however the National Cyber Security Centre has helpful guidance available **Mitigating malware and ransomware attacks - NCSC.GOV.UK**

REPORTING CYBER CRIME

If you fall victim to fraud or cyber crime, you can report this to Action Fraud by visiting www.actionfraud.police.uk or by calling 0300 123 2040.

If you have received an email that you're not sure about, you can report this to the **National Cyber Security Centres Suspicious Email Reporting Service (SERS)**. Simply forward the email to **report@phishing.gov.uk**.

The SERS automatically analyses suspicious emails and, if it considers it to be malicious, can take steps to have email accounts and associated websites closed down, meaning each report can really make a difference.

DORSET POLICE

Dorset Police
Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

E cybercrimeprevention@dorset.pnn.police.uk
www.dorset.police.uk

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

Office of the Dorset Police & Crime Commissioner
Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

T 01202 229084
E pcc@dorset.pnn.police.uk
www.dorset.pcc.police.uk