CYBER CRIME NEWS

ISSUE 3 • MARCH 2023

WELCOME TO CYBER CRIME NEWS

Welcome to the March 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.

The March issue will:

- Provide advice on how to avoid tax year end scams
- Explain wiper malware and how to protect your business against it by using backups
- Provide useful hints and tips and how to access training

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

PRODUCED BY DORSET OPCC AND DORSET POLICE

DORSET POLICE

AVOID THE TAX YEAR END SCAMS

Fraudsters are ever inventive when it comes to turning current events into opportunities to scam people, and the end of the financial year is no exception.

After all, businesses may well be expecting to hear from HMRC or, at least, they might not find it too suspicious if they did.

For this reason, you need to be wary of potential scams as the financial year comes to an end. Be cautious around unexpected emails and phone calls – it is highly likely that fraudsters will use phishing emails to lure unsuspecting people in to handing over sensitive information. Whilst they are usually easier to detect, telephone scams are also prevalent. Be sure to check emails thoroughly before taking action.

Here are a few of our top tips to protect you and your business at this time:

1. **Check the sender's email address -** It is easy for criminals to create lookalike accounts and give themselves legitimate sounding display names. Genuine HMRC email addresses should end with **@hmrc.gov.uk**. Anything different, even a slight variation, is highly likely a scam.

2. **Check the links before you click them -** It is easy to mask where a link will take you. Criminals can embed malicious links in buttons or hyperlinks or may even design them to look like a known trusted link. Before you click, hover your cursor over the link. This will cause the true destination of that link to appear either in a box next to the cursor, or at the bottom of your screen.

3. **Be wary of vague or generic greetings -** HMRC will usually address you personally, or at least someone with financial responsibility within your organisation. If you receive an email with a vague greeting such as "Dear Sir / Madam", be suspicious.

4. **Report anything that you are not sure about** to the Suspicious Email Reporting Service (SERS), by forwarding it to **report@phishing.gov.uk**. This automated service analyses emails, including the sender's address and any links within and, if it is deemed malicious, will take steps to have the accounts and websites removed from the internet.

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

PRODUCED BY DORSET OPCC AND DORSET POLICE

DORSET POLICE

PICK OF THE MONTH

In each edition we will provide you with a common type of cybercrime and explain what it is, why it is a threat and what you can do to protect yourself against it.

WIPER MALWARE

Does your business backup data?

What is a backup and why should you be doing them?

Since the start of the war in Ukraine in 2022, a particular type of malware has risen in prominence.

Known as wiper malware, it seeks to wipe a system clean of data. Wiper malware is nothing new and has not previously been popular among criminals owing to the fact it is harder to monetise. That said, its application as a weapon is clear, and criminal groups have begun offering wiper malware as a service, with a major security vendor noting a 53% increase in wiper malware activity between Quarter 3 and Quarter 4 2022.

With other threats, such as Ransomware, covered in January's e-newsletter, a victim is left with encrypted data which leaves them at least a small chance at being able to recover their data. Wiper malware is fully destructive, leaving nothing behind. Having a second, or even third copy of your company data is relatively simple to achieve and can negate the most severe consequences of a wiper malware attack.

So, how do you backup your data?

Identify what data you need to backup – Consider what information your business could not function without. Customer details, orders, quotations and payment details, for instance. These are often stored in a handful of common folders on a device or network, though could easily be backed up to a hard drive, or the cloud.

Determine how regularly you should backup – The best solution is to backup your data at least every day. That way should the worst happen, you will only lose one days' worth of data.

Keep your backups separate - USB sticks and hard drives are a great solution, depending on the volume of data you need to store. Cloud storage is also a great choice, particularly for large volumes of data. It is important to ensure that backups can only be accessed by approved people, and that they are not permanently connected to the device or network that stores the original copy – ransomware can often move to attached storage, potentially encrypting your back up too.

Choose a reputable provider – If you opt for cloud storage, be sure that you choose a vendor that you trust. Utilising the services of a specialist means you can benefit from security expertise that might otherwise be cost prohibitive.

Make data backup part of your daily business – It might seem inconvenient, but it is far easier than trying to recover lost data without a backup. Many solutions allow you to set up automated backups, meaning new files of certain types can be saved to specified folders in the cloud, or your chosen physical media.

Further advice about backing up your data can be found in the NCSC Small Business Guide: Cyber Security - https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data

If you think your organisation would benefit from Cyber Awareness training, including how to spot phishing emails and other scams, get in touch by emailing cybercrimeprevention@dorset.pnn.police.uk

HELPFUL ADVICE

Wiper malware 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