The fight against cybercrime

Large Corporate OMB

03 November 2021

Simon Cubitt explains the range of cybercrimes threatening those working in tax, and gives some practi cal advice about how to prevent fraud

Key Points

What is the issue?

In a few simple steps, businesses can significantly increase their levels of protection against the most common types of cybercrime, reducing not only the chances of being affected, but the potential impact of any attack.

What does it mean for me?

Taking steps to protect your business against ransomware attacks will help to increase resilience against a number of other attacks known to affect tax agents, their HMRC tax accounts and their clients.

What can I take away?

Exercise in a Box (see bit.ly/3mwnNbk) is an online tool from the NCSC which helps organisations to test and practise their response to a cyberattack. It is free and you don’t have to be an expert to use it.

Ensuring that you’re operating securely in cyber space can be a daunting prospect, but there’s plenty of advice and guidance available to help you make sure you’re getting it right.

HMRC works closely with and recommends advice provided by the National Cyber Security Centre (NCSC), a government organisation delivering clear, quality guidance to individuals and businesses to help them protect their data, assets and reputation.

In a few simple steps, businesses can significantly increase their levels of protection against the most common types of cybercrime, reducing not only the chances of being affected, but the potential impact of any attack.

This article focuses on ransomware, a threat that can have a big impact on businesses and something we hear about regularly here at HMRC.

Access to IT and data is vital to many individuals and organisations in the modern era, particularly so in accountancy work. Ransomware is software which denies victims access to their data by locking it away and, as the name suggests, demanding a ransom to release the digital key.

Increasingly, criminals will also publish stolen data if the victim refuses to pay, exposing sensitive information and risking reputations.

For tax advisors and HMRC, these attacks represent serious risks to the sensitive financial information of clients, in turn increasing the risk to them of reputational damage, impersonation and fraud.

Taking steps to protect your business against ransomware attacks will also help to increase resilience against a number of other attacks known to affect tax agents, their HMRC tax accounts and their clients.

Ransomware operators rely on a range of vulnerabilities to be able to run their malicious software.

We will begin by looking at two common ways they invade victim systems: remote administration services; and email.

Remote administration

Many businesses worldwide take advantage of remote administration tools. These enable users to remotely connect to a PC or server over the internet, providing full access to the data and software on it. IT support might use these services remotely to fix system issues, or tax advisors to connect to their office PC, allowing them to access records while at a client site.

Unfortunately, attackers target users like these to obtain or simply guess their login details for these services. The most popular remote access tool is the Windows Remote Desktop Protocol (RDP), and the compromise of RDP accounts is the source of about 50% of ransomware attacks.
Some businesses might be unaware they are even running these remote desktop services. For example, they could have been set up for a specific IT project or to avoid coming into the office over a weekend, but long forgotten and not switched off .

The NCSC provides an Early Warning Service (EWS) (see bit.ly/3Bf1rRw), a free facility to warn about potential cyberattacks as early as possible against your internet domain or static IP address. The NCSC collates information from commercial data feeds and provide alerts if:

- a system on your network is likely to have been infected with a strain of malware;
- there are indications that your assets have been associated with malicious or undesirable internet activity; or
- your internet-exposed systems have vulnerabilities or open ports, including RDP services.

If you don’t need RDP, it is best to disable it. If you do need it, you must ensure you have strong passwords on those accounts allowed to use it, and multi-factor authentication is recommended.

The important consideration with passwords is that they should be unique (different on different websites and computers) and hard to guess. The NCSC recommends that you create a strong password by thinking of three random words. The centre also provides guidance for organisations on implementing multi-factor authentication, covering what it protects against, when to use it, and what types of extra authentication to consider (see bit.ly/3mrTq5K).

HMRC has supported accountants who have been compromised through their remote administration services. Victims have reported the mouse moving of its own accord, while other attackers have disabled the local screen to hide their activity or timed their next steps outside office hours.
Attacker objectives include altering invoices to clients to divert payments, theft of client records to impersonate them in fraud, and modifying client tax records for financial gain.

Many web browsers offer to remember usernames and passwords to online accounts, so an attacker with remote access could use these to gain access to other online services too. You can check in your browser setting for a list of the web accounts that might be at risk and you should prioritise changing those passwords. If you think your HMRC account has been compromised, you should change your password promptly, ideally using a different device, and contact HMRC.

Phishing email

Another common method for delivering many types of malicious software, including ransomware, is email. These typically contain a lure to tempt the user to click a link or open a malicious attachment. In addition to email, the starting point could also be via text message, social media or a phone call to direct the victim to a malicious site.

More sophisticated attackers employ techniques to convince targets to act including:

- Urgency: specifying a tight deadline to act so you don’t take time to consider it;

- Authority: presenting the message as from a trusted sender, such as a colleague or associate;
- Mimicry: exploiting user's daily patterns by sending similar messages about the time they'd expect them; and
- Curiosity: attackers might try to entice users in.

The Centre for the Protection of National Infrastructure (CPNI) and NCSC have developed a Don't Take the Bait! campaign (see bit.ly/3DchUqf), providing free resources to support organisations in raising awareness of phishing among their teams.

Over the years, it has not been uncommon for phishing emails to mimic official HMRC contacts. HMRC takes a proactive approach to protect the UK public when attackers misuse our brand. Our tactics have pushed HMRC from the third most abused brand globally in 2015 to well outside of the top 100 now.

In the last year HMRC has:

- responded to 998,485 referrals of suspicious contact from the public. Some 440,729 of these offered bogus tax rebates;
- worked with the telecoms industry and Ofcom to remove 2,020 phone numbers being used to commit HMRC-related phone scams;
- responded to 413,527 reports of phone scams in total, 92% up on the previous year;
- reported more than 12,705 malicious web pages for takedown;
- detected 463 Covid-related financial scams since March 2020, most by text message; and
- asked Internet Service Providers to take down 443 Covid-related scam web pages.

> There are many ways an organisation can defend against phishing and its consequences, including strong passwords and multi-factor authorisation.

HMRC also automatically identifies more than 50% of HMRC-branded cyber scams before members of the public have even reported them to it. It deploys innovative technologies to prevent misleading and malicious communications ever reaching our citizens; and warns the public by sharing details and examples of genuine and scam

communications on GOV.UK (see bit.ly/3oArPlA).

A wide range of brands and lures are used to deceive and dupe victims. The important thing is to think before you click. If you're not sure a message is genuine, verify the communication (without replying). HMRC and other organisations provide online guidance on how to spot fake messages, often with examples (see bit.ly/3izejdT).

There are many ways an organisation can defend against phishing and its consequences, and you can learn more on the NCSC website (see bit.ly/3uFtWFI). These include using strong passwords and multi-factor authorisation. Such controls are especially important for online business software suites, such as Office 365 or Google Workspace, where a range of other services and files can be compromised in addition to email.

Cyberattacks have been known to give criminals access to tax advisors' files through such compromised accounts.

Loss of control of an email account can leave you vulnerable to attacks that exploit typical password recovery processes on online accounts, when a reset link can be requested to the registered email account. If you find you are unable to access your HMRC account with your credentials and suspect you might have had a security problem with your email account, make sure you contact HMRC immediately. When a victim takes the bait and mistakenly runs the malicious software, an attacker gains access to the computer. From here, they can begin their ransomware attack.

Ransomware

Once an attacker accesses a system, they can explore files, consider what the victim can afford to pay, locate and disable any backups, and copy and encrypt data. The first sign of an issue for users might be an on-screen message, giving instructions for how to pay the ransom to regain access to their data.

It's increasingly common for copies of the files to be taken so that they can be publicly released online, meaning there will be further consequences for victims if demands are not met. Not only do files become inaccessible but confidentiality is compromised, with the associated potential reputational and regulatory impacts.

Loss of control of an email account can leave you vulnerable to attacks that exploit typical password recovery processes on online accounts.

The important actions you can take to help prepare for such attacks are to:

- make regular backups;
- take steps to prevent malware from being delivered and spreading to devices;
- take steps to prevent malware from running on devices; and
- prepare for an incident.

The NCSC provides detailed advice on each of these steps in its guidance on Mitigating Malware and Ransomware Attacks (see bit.ly/3DsmyAP).

This also includes recommended steps to take if you are already infected, to limit the impact. Backups are important to recover the data your business relies upon if you become a victim, but attackers know this too, and backups are often targeted if they're accessible. The NCSC advises on protecting your backups from attackers (see bit.ly/2ZSU0Sh).

Next steps and further resources Many businesses might feel confident that they have the controls and processes in place, but a good way of making sure is to test them.

Exercise in a Box (see bit.ly/3mwnNbk) is an online tool from the NCSC which helps organisations to test and practise their response to a cyberattack. It is free and you don't have to be an expert to use it.

The service provides exercises, based around the main cyber threats, which your organisation can carry out in your own time, in a safe environment, as often as you want. It includes everything you need for setting up, planning, delivery and post-exercise activity, all in one place.

We've discussed the key steps organisations should consider to protect the devices and services they rely upon. The NCSC provides tailored advice for different-sized organisations, from the individual to large groups. Tax advisors might also find the guidance for small to medium-sized organisations particularly relevant (see bit.ly/2WIWhhR).