

The impact of Covid-19

Cyber Security

IN PARTNERSHIP WITH



POLICE
SCOTLAND
Keeping people safe
POILEAS ALBA



**Scottish Business
Resilience Centre**

What is Cyber security.

Cyber security is the means by which individuals and organisations reduce the risk of becoming victims of cyber-attack.

Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work - from theft or damage. It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online.

It's more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data, and devices. Here are some examples of how the Pandemic has enabled SOC to exploit the cyber security of SMEs and some useful prevention solutions.

Covid-19 exposes UK's cyber security vulnerabilities – with 65,000 attacks taking place daily

UK SME's are at risk of 65,000 cyber security attacks daily – with around 4,500 of these being successful – and the figure could be much higher since the beginning of Covid. Lockdown measures forced a change to businesses working practices overnight, where just 11% of UK businesses stated their entire workforce were able to work remotely pre-lockdown, rose to 70% once lockdown hit. Of the 70%, over half (53%) of these firms were able to transition to remote working in less than 48 hours. Half of companies (48%) admitted that they do not have adequate cyber security provision to maintain a 100% remote working model. Although robust practices and enhanced customer trust is still

important, it is remote working that that has shone a spotlight on the issue of cyber security. SMEs should act fast before they are faced with the consequences of personal information being mishandled from temporary 'off site' offices.



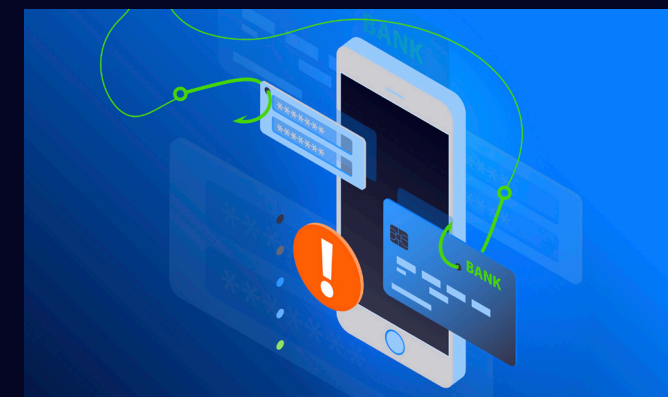
SME Alert from SBRC in conjunction with Police Scotland

Cyber criminals will be using COVID-19 to increase their activities to attack organisations and private individuals. The National Cyber Security Centre has reported increased criminal activity aiming to obtain money from victims using fear of COVID-19 as a tactic. Many illicit actors are engaged in fraudulent schemes that exploit vulnerabilities created by the pandemic. This section contains descriptions of COVID-19-related malicious cyber activity and scams. This SME alert addresses the primary means by which cybercriminals and malicious state actors are increasingly exploiting the COVID-19 pandemic in cyber-enabled crime through malware and phishing schemes, extortion, business mandate fraud, and exploitation of remote applications.

The significant migration toward remote access in the pandemic environment presents opportunities for criminals to exploit institutions' remote systems and customer-facing processes. Cyber criminals and malicious state actors are targeting vulnerabilities in remote applications and virtual environments to steal sensitive information, compromise financial activity, and disrupt business operations.

Specific information for SMEs is available at [NCSC Small-Medium Business Site](#) and from the [Scottish Government Cyber Resilience report](#)

A recent [Interpol report](#) highlighted; Threat actors have revised their usual online scams and phishing schemes. By deploying COVID-19 themed phishing emails, often impersonating government and health authorities, cybercriminals entice victims into providing their personal data and downloading malicious content. Around two-thirds of member countries which responded to the global cybercrime survey reported a significant use of COVID-19 themes for phishing and online fraud since the outbreak. The [Europol Covid response report](#) further highlights these emerging trends.



Targetted Phishing Campaigns

Law enforcement have observed significant increases in broad-based and targeted phishing campaigns that are attempting to lure companies, especially healthcare and pharmaceutical providers, with offers of COVID-19 information and supplies. Phishing scams target individuals with communications appearing to come from legitimate sources to collect victims' personal and financial data and potentially infect their devices by convincing the target to download malicious programs. Some phishing emails lure victims via domain names that mimic names of organizations. In January a number of spam or phishing emails emerged that referenced COVID-19 but by early March they represented a significant percentage of all malicious traffic. In addition, an increasing number of malicious websites are being created using the coronavirus, or related terms with over 42,000 sites being registered since early February. Law enforcement agencies have disrupted hundreds of malicious domains used to exploit the pandemic. Whatever your business, however big or small it is, you will receive phishing attacks at some point.

Common phishing emails

Common phishing emails relate to a number of special offers such as:

- Commercial organisations offering free medical products, trials or a coronavirus cure.
- Tax refund support or the offer of financial aid from the UK Government.
- Safety advice from the World Health Organisation.
- Home working and contacts from bogus HR Departments.
- Extortion requests demanding payment or confidential information will be released.

General guidance is available at [National Cyber Security Centre Phishing infographic](#)

Mandate fraud is one of the most reported frauds in the UK.



BUSINESS MANDATE FRAUD

Cybercriminals have increasingly exploited the COVID-19 pandemic by using Mandate Fraud schemes. A common scheme involves criminals convincing companies to redirect payments to new accounts, while claiming the modification is due to pandemic-related changes in business operations. Criminals often use spoofed or compromised email accounts to communicate these urgent, last-minute payment changes. In the COVID-19 environment, criminals insert themselves into communications by impersonating a critical player in a business relationship or transaction, to intercept or fraudulently induce a payment for critically needed supplies. Interpol have projected Business Mandate Fraud shall likely surge due to the economic downturn and shift in the business landscape, generating new opportunities for criminal activities. Extra awareness is needed to defeat these attacks. We must not become complacent in these unprecedented and challenging times when perhaps our focus is elsewhere. General guidance is available at [Mandate Fraud Guidance](#)

COVID-19 PPE MANDATE FRAUD CASE STUDY

An international supplier of personal protective equipment had their email compromised by organized criminals, who then used this data to contact the UK supplier, and request a change of bank account details for payment prior to shipping. The UK supplier was about to pay for vital equipment for the NHS, but became suspicious and sought further advice. By following general bank mandate fraud prevention guidance, their actions prevented the fraudulent payment being processed. The details of this attempt fraud were shared with law enforcement authorities and in turn with other organisations to increase vigilance and help prevent this type of fraud.

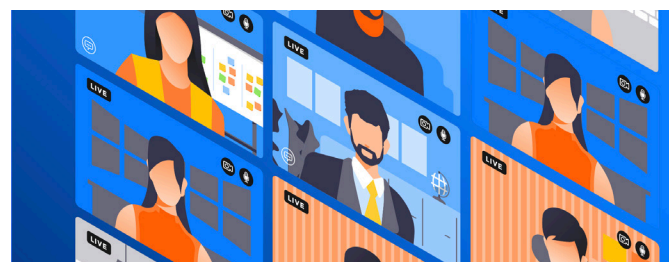


MALICIOUS DOMAINS

Taking advantage of the increased demand for supplies and information on COVID-19, there has been a significant increase of cybercriminals registering domain names containing keywords, such as "coronavirus" or "COVID". These fraudulent websites underpin a wide variety of malicious activities including C2 servers, malware deployment and phishing. From February to March 2020, a 569 per cent growth in malicious registrations, including malware and phishing and a 788 per cent growth in high-risk registrations were detected and reported to Law Enforcement by a private sector partner.

Microsoft took legal action in July 2020 to seize several malicious domains that were used by cybercriminals exploiting the Covid and Coronavirus domain names in extensive phishing and Business Email Compromise attacks on Office 365 accounts amid the current pandemic.

VIDEO CONFERENCING



The COVID-19 lockdown means many organisations are using home-working on a greater scale. With more staff now working remotely, video conferencing has an obvious role to play. This guidance helps organisations to select, configure and securely implement video conferencing services. This emerging threat is popular for criminals, with a number of new scams emerging online in recent weeks. The scams include phishing attacks to steal user login details, allowing hackers' access into a company's network to cause havoc and spread malware. General guidance on video conferencing is available at [The National Cyber Security Centre](#).

PREVENTION

What cyber security actions have you undertaken to protect your business? Failure to prepare may result in cyber criminals obtaining business critical data, personal data, damage to your IT network, reputational damage to your company and even much needed grant funding being applied by fraudsters in your or your company details.

Checklist for SMEs to mitigate cyber attacks:

1. Passwords

Always change your default passwords for all systems to something new that cannot be easily guessed and make sure you use unique passwords for each of your systems.

2. Security software

Security software helps protect your business against malicious or otherwise unauthorised network traffic.

3. Staff

Tempting someone to access malicious attachments and websites is a common technique to install malicious codes onto a computer and compromise a network. Educate your staff to be wary of unsolicited emails and attachments.

4. Responsibility

Many small businesses do not have a dedicated IT manager. Where this is the case, appointing a person with day-to-day responsibility for cyber security is highly recommended.

5. Software patches

Keep software patches up-to-date and use supported versions of software. This is important to guard against malware infiltrating computers. Every time you leave any program unpatched, you're leaving the door ajar for a cyber-attack.

6. Backup

Make sure you backup your critical data on a regular basis (daily, weekly or monthly) with both offline copies as well as offsite storage of at least the weekly backup data. This ensures you have access to your information in the event a cyber security incident.

7. Non-administrator accounts

Administrator level accounts are targeted by attackers because they provide potentially full access to your system. By creating non-administrator level accounts and using them for day-to-day activities, you reduce the risk of network compromise.

8. Remote access

Staff with remote access can be targeted by attackers attempting to gain access to your network. To make remote access more secure, use 'allow listing' and strong passwords. Also secure other public-facing services such as your web server, through activities such as independent website testing for vulnerabilities.

9. Critical information

Controlling physical access to data minimises the risk of theft, destruction or tampering. So does using encryption when this information is stored on portable devices or removable media.

10. Logs

Malicious behaviour is more likely to be detected if you automatically log information relating to network activities and computer events. Best practice is to retain these logs and regularly review them for changes to normal behaviour.


General Cyber related guidance is available at;

[CEO Fraud Guidance](#)
[Nation Cyber Security Centre Home-Working guidance](#)
[Grant Fraud Guidance](#)
[National Cyber Security Centre Ransomware Guidance](#)
[Health & Safety Executive](#)



Scottish Business Resilience Centre

 Oracle Campus
Blackness Road
Linlithgow
West Lothian
EH49 7LR

 01786 447 441

 enquiries@sbrcentre.co.uk

 www.sbrcentre.co.uk

 @SBRC_Scotland

A Company Limited by guarantee and registered in Scotland
No. SC170241 | VAT Registration Number: 717 2746 27

IN PARTNERSHIP WITH



**POLICE
SCOTLAND**
Keeping people safe
POILEAS ALBA

