National Cyber Security Centre
a part of GCHQ

CISA
CYBER+INFRASTRUCTURE

Advisory: COVID-19 exploited by malicious cyber actors

Version 1.0

8th April 2020

This is a joint advisory from the United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Introduction

This advisory provides information on exploitation by cyber criminal and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic. It includes a non-exhaustive list of indicators of compromise (IOCs) for detection as well as mitigation advice.

COVID-19 exploitation

An increasing number of malicious cyber actors are exploiting the current COVID-19 pandemic for their own objectives. In the UK, the NCSC has detected more UK government branded scams relating to COVID-19 than any other subject. Although, from the data seen to date, the overall levels of cyber crime have not increased both the NCSC and CISA are seeing a growing use of COVID-19 related themes by malicious cyber actors. At the same time, the surge in home working has increased the use of potentially vulnerable services, such as Virtual Private Networks (VPNs), amplifying the threat to individuals and organisations.

APT groups and cyber criminals are targeting individuals, small and medium businesses and large organisations with COVID-19 related scams and phishing emails. This advisory provides you with an overview of COVID-19 related malicious cyber activity. It offers practical advice that individuals and organisations can follow to reduce the risk of being affected. The IOCs provided within the accompanying .csv and .stix files of this advisory are based on analysis from CISA, NCSC, and industry.

Note: this is a fast-moving situation and this advisory does not seek to catalogue all COVID-19 related malicious cyber activity. You should remain alert to increased activity relating to COVID-19 and take proactive steps to protect yourself and your organisation.

Summary of attacks

APT groups and cyber criminals are exploiting the COVID-19 pandemic as part of their cyber operations. These cyber threat actors will often masquerade as trusted entities. Their activity includes using coronavirus-themed phishing messages or malicious applications, often masquerading as trusted entities that may have been previously compromised. Their goals and targets are consistent with long-standing priorities such as espionage and information operations.

Cyber criminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware.

Both APT groups and cyber criminals are likely to continue to exploit the COVID-19 pandemic over the coming weeks and months. Threats observed include:

- Phishing, using the subject of coronavirus or COVID-19 as a lure
- Malware distribution using coronavirus or COVID-19 themed lures
- Registration of new domain names containing coronavirus or COVID-19 related wording
- Attacks against newly (and often rapidly) deployed remote access or remote working infrastructure.

Social engineering techniques

Malicious cyber actors rely on basic social engineering methods to entice a user to carry out a specific action. These actors are taking advantage of human traits such as curiosity and concern around the coronavirus pandemic in order to persuade potential victims to:

- Click on a link or download an app that may lead to a phishing website, or the downloading of malware, including ransomware.
    - For example, a malicious Android app purports to provide a real-time coronavirus outbreak tracker but instead attempts to trick the user into providing administrative access to install 'CovidLock' ransomware on their device.[1]
- Open a file (such as an email attachment) which contains malware.
    - For example, email subject lines contain COVID-19 related phrases such as 'Coronavirus Update' or '2019-nCov: Coronavirus outbreak in your city (Emergency).'

To create the impression of authenticity, malicious cyber actors may spoof sender information in an email to make it appear to come from a trustworthy source, such as the World Health Organization (WHO) or an individual with 'Dr.' in their title. In several examples, actors send phishing emails that contain links to a fake email login page. Other examples purport to be from an organisation's human resources (HR) department and advise the employee to open the attachment.

Malicious file attachments containing malware payloads may be named with coronavirus or COVID-19 related themes, such as "President discusses budget savings due to coronavirus with Cabinet.rtf."

Note: A non-exhaustive list of IOCs related to this activity is provided within the accompanying .csv and .stix files linked to this advisory.

[1] https://www.techrepublic.com/article/covidlock-ransomware-exploits-coronavirus-with-malicious-android-app/

Phishing

The NCSC and CISA have both observed a large volume of phishing campaigns which use the social engineering techniques described above.

Examples of phishing email subject lines include:

- 2020 Coronavirus Updates
- Coronavirus Updates
- 2019-nCov: New confirmed cases in your City
- 2019-nCov: Coronavirus outbreak in your city (Emergency).

These emails will contain a call to action encouraging the victim to visit a URL that malicious cyber actors use for stealing valuable data, such as usernames and passwords, credit card information and other personal information.

SMS Phishing

Most phishing attempts come by email but the NCSC and CISA have observed some attempts to carry out phishing by other means, including text messages (SMS).

Historically, SMS phishing has often used financial incentives, including government payments and rebates (such as a tax rebate) as part of the lure. Coronavirus-related phishing continues this financial theme, particularly in light of the economic impact of the epidemic and governments' employment and financial support packages.

For example, a series of SMS messages uses a UK government themed lure to harvest email, address, name, and banking information. These SMS messages, purporting to be from 'COVID' and 'UKGOV,' (see figure 1) includes a link directly to the phishing site (see figure 2).

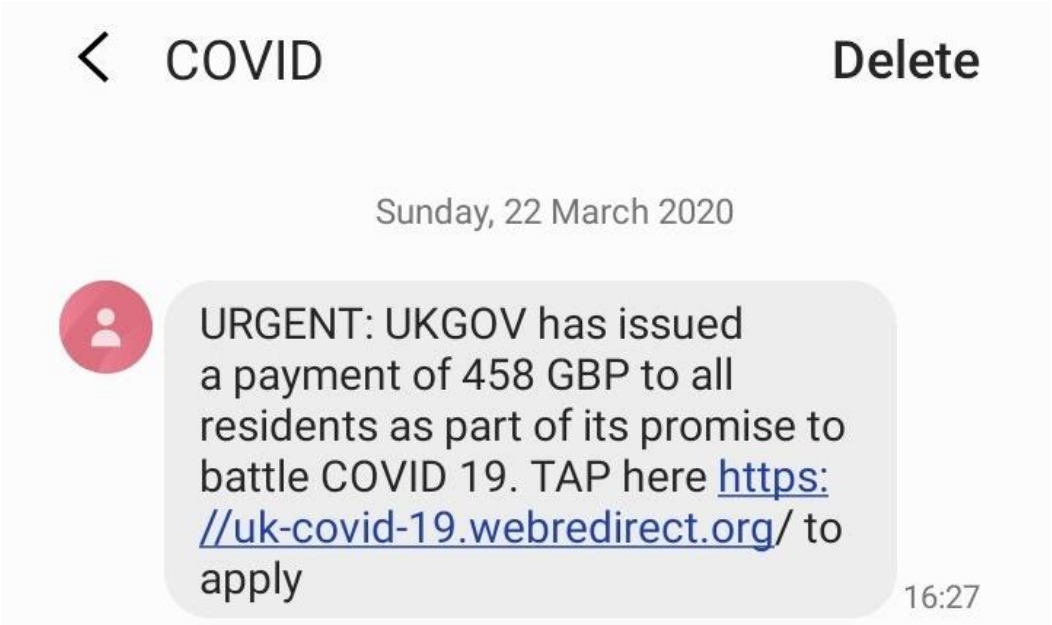

Figure 1 – UK Government themed SMS phishing

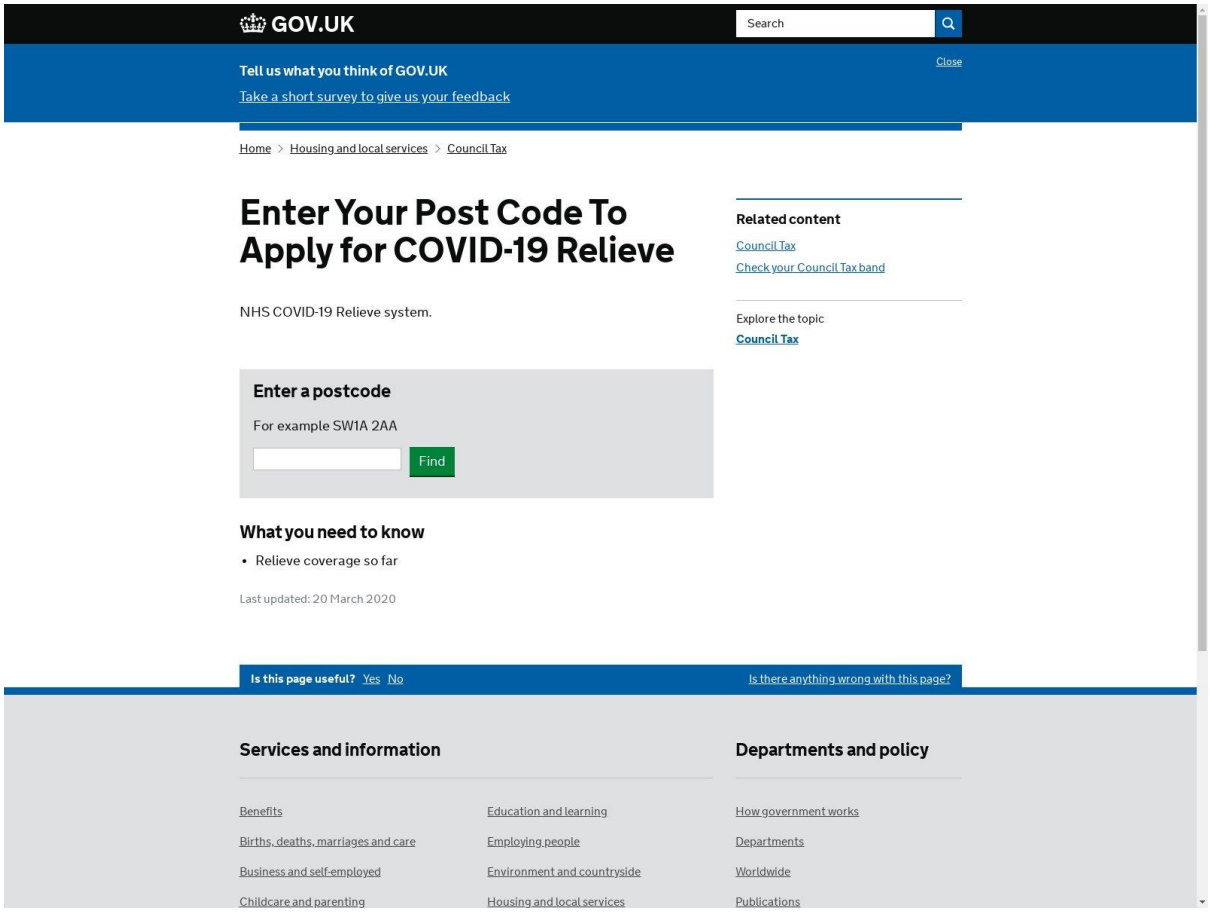

Figure 2 - UK Government themed phishing page

As this example demonstrates, malicious messages can arrive by methods other than email. In addition to SMS, possible channels include WhatsApp and other messaging services. Malicious cyber actors are likely to continue using financial themes in their phishing campaigns. Specifically, it is likely that they will use new government compensation schemes responding to COVID-19 as themes in phishing campaigns.

Phishing for credential theft

A number of actors have used COVID-19 related phishing to steal user credentials. These emails will include previously mentioned COVID-19 social engineering techniques, sometimes complemented with urgent language to enhance the lure.

If the user clicks on the hyperlink, a spoofed login webpage appears which includes a password entry form. These spoofed login pages may relate to a wide array of online services including - but not limited to - email services provided by Google or Microsoft, or services accessed via government websites.

To further entice the recipient, the websites will often contain COVID-19 related wording within the URL (for example, ‘corona-virus-business-update,’ ‘covid19-advisory’ or ‘cov19esupport’). These spoofed pages are designed to look legitimate or

accurately impersonate well-known websites. Often the only way to notice malicious intent is through observing the website URL. In some circumstances, malicious cyber actor specifically customise these spoofed login pages for the intended victim.

If the victim enters their password on the spoofed page, the attackers will be able to access the victim's online accounts such as their email inbox. This access can then be used to acquire personal or sensitive information, or to further disseminate phishing emails, using the victim's address book.

Phishing for malware deployment

A number of threat actors have used COVID-19 related lures to deploy malware. In most cases, actors craft an email that persuades the victim to open an attachment or download a malicious file from a linked web page. When they open the attachment the malware is executed, compromising the victim's device.

For example, the NCSC has observed various email distributed malware which deploys the Agent Tesla keylogger malware. The email appears to be sent from Dr Tedros Adhanom Ghebreyesus, Director-General of the World Health Organization (WHO). This email campaign began on Thursday, March 19, 2020. Another similar campaign offers thermometers and face masks to fight the epidemic. The email purports to attach images of these medical products but instead contains a loader for Agent Tesla.

In other campaigns, emails included an Excel attachment (e.g. '8651 8-14-18.xls') or contained URLs linking to a landing page that – if clicked - redirects to download an Excel document such as 'EMR Letter.xls.' In both cases, the Excel file contains macros that, if enabled, execute an embedded dynamic-link library (DLL) to install the Get2 loader malware. Get2 loader has been observed loading the GraceWire Trojan.

The TrickBot malware has been used in a variety of COVID-19 related campaigns. In one example, emails target Italian users with a document purporting to be information related to COVID-19 (see figure 3). The document contains a malicious Macro which downloads a batch file (BAT) which launches JavaScript, which - in turn - pulls down the TrickBot binary, executing it on the system.

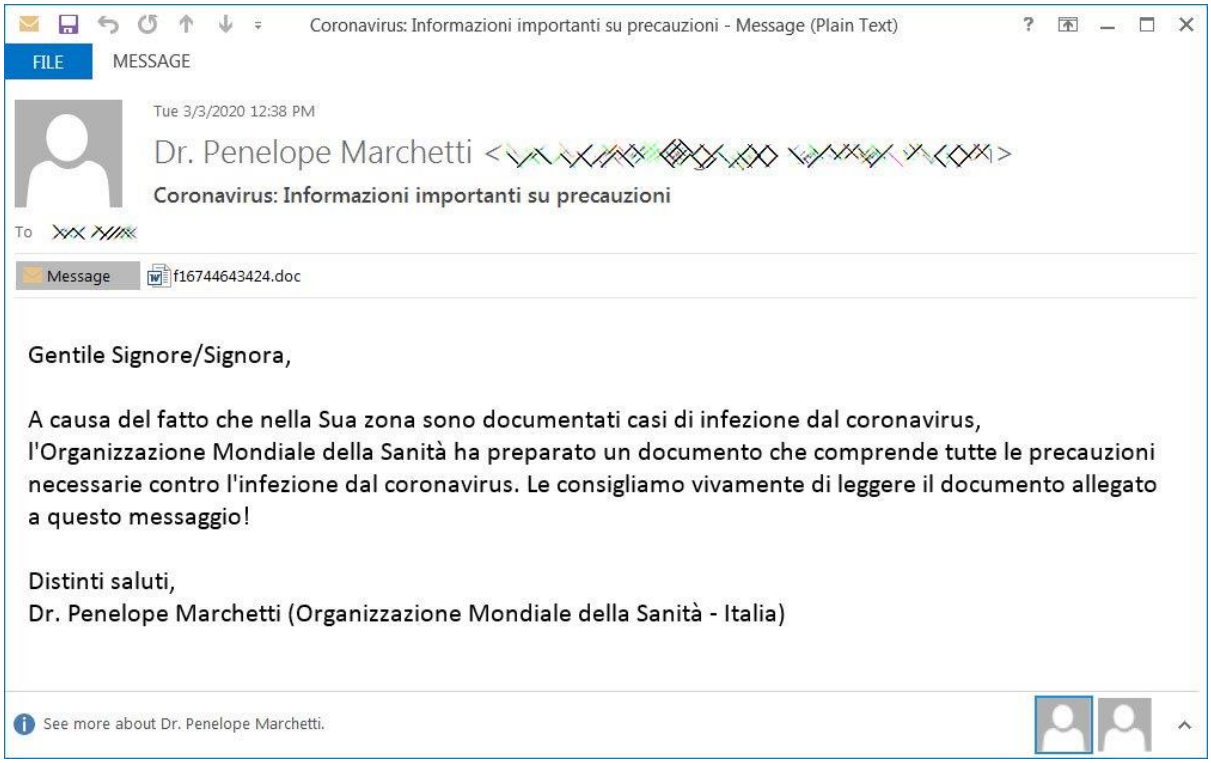

Figure 3 – Email containing malicious macro targeting Italian users[2]

In many cases, Trojans - such as Trickbot or GraceWire2 - will download further malicious files such as Remote Access Trojans (RATs), desktop-sharing clients and ransomware. In order to maximise the likelihood of payment, cyber criminals will often deploy ransomware at a time when organisations are under increased pressure. Hospitals and health organisations in the United States,[3] Spain[4] and across Europe[5] have all been recently affected by ransomware incidents.

As always, you should be on the lookout for new and evolving lures. Both the NCSC[6] and CISA[7,8] provide guidance on mitigating malware and ransomware attacks.

Exploitation of new home working infrastructure

Many organisations have rapidly deployed new networks, including VPNs and related IT infrastructure, to cater for the large shift towards home working.

Malicious cyber actors are taking advantage of this on this mass move to home working by exploiting a variety of publicly known vulnerabilities in VPNs and other remote working tools and software. In several examples, the NCSC and CISA have

[2] https://www.bleepingcomputer.com/news/security/trickbot-malware-targets-italy-in-fake-who-coronavirus-emails/
[3] https://securityboulevard.com/2020/03/maze-ransomware-continues-to-hit-healthcare-units-amid-coronavirus-covid-19-outbreak/
[4] https://www.computing.co.uk/news/4012969/hospitals-coronavirus-ransomware
[5] https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/
[6] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
[7] https://www.us-cert.gov/ncas/tips/ST18-271
[8] https://www.us-cert.gov/Ransomware

observed actors scanning for publicly known vulnerabilities in Citrix. Citrix vulnerability (CVE-2019-19781) and its exploitation has been widely reported online, since early January 2020. Both the NCSC[9] and CISA[10] provide guidance on CVE-2019-19781 and continue to investigate multiple instances of this vulnerability's exploitation.

Similarly known vulnerabilities affecting VPN products from vendors Pulse Secure, Fortinet and Palo Alto continue to be exploited. CISA provides guidance on the Pulse Secure vulnerability[11] and the NCSC provides guidance on the vulnerabilities in Pulse Secure, Fortinet, and Palo Alto.[12]

Malicious cyber actors are also seeking to exploit the increased use of popular communications platforms (such as Zoom or Microsoft Teams) by sending phishing emails that include malicious files with names such as 'zoom-us-zoom_##########.exe' and 'microsoft-teams_V#mu#D_##########.exe' (# representing various digits that have been reported online).[13] The NCSC and CISA have also observed phishing websites for a number of popular communication platforms. In addition, attackers have been able to hijack teleconference and online classrooms that have been set up without security controls (e.g. passwords) or with unpatched versions of the communications platform software.[14]

The surge in home working has also led to an increase in the use of Microsoft's Remote Desk Protocol (RDP). Attacks on unsecured RDP endpoints (i.e. exposed to the internet) are widely reported online,[15] and recent analysis[16] has identified a 127% increase in exposed RDP endpoints. The increase in RDP use could potentially make IT systems, without the right security measures in place, more vulnerable to attack.[17]

Indicators of compromise

The NCSC and CISA are working with law enforcement and industry partners to disrupt or prevent these malicious COVID-19 themed cyber activities. We have published a non-exhaustive list of COVID-19 related IOCs via the following links:

- CSV file: https://www.us-cert.gov/sites/default/files/publications/AA20-099A_WHITE.csv
- Stix File: https://www.us-cert.gov/sites/default/files/publications/AA20-099A_WHITE.stix.xml

[9] https://www.ncsc.gov.uk/news/citrix-alert
[10] https://www.us-cert.gov/ncas/alerts/aa20-031a
[11] https://www.us-cert.gov/ncas/alerts/aa20-010a
[12] https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities
[13] https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/
[14] https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic
[15] https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ and
[16] https://blog.reposify.com/127-increase-in-exposed-rdps-due-to-surge-in-remote-work
[17] https://www.us-cert.gov/ncas/tips/ST18-001

In addition, there are a number of useful resources online, which provide details of COVID-19 related malicious cyber activity:

- Recorded Futures' report, Capitalizing on Corona Panic, Threat Actors Target Victime worldwide
- DomainTools' Free COVID-19 Threat List – Domain Risk Assessments for Coronavirus Threats
- GitHub list of IOCs used in COVID-19 related cyberattack campaigns, gathered by GitHub user, Parth D. Maniar
- GitHub list of Malware, spam, and phishing IOCs that involve the use of COVID-19 or coronavirus gathered by SophosLabs
- Reddit master thread to collect intelligence relevant to COVID-19 malicious cyber threat actor campaigns
- Tweet regarding the MISP project's dedicated #COVID2019 MISP instance to share COVID-related cyber threat information

Conclusion

Malicious cyber actors are continually adjusting their tactics to take advantage of new situations, and the COVID-19 pandemic is no exception. Malicious cyber actors are using the high appetite for COVID-19 related information as an opportunity to deliver malware and ransomware and to steal user credentials. Individuals and organisations should remain vigilant. For genuine information about the virus, please use trusted resources such as the UK government website[18], Public Health England[19] or NHS websites[20].

Mitigating the risk

Following the NCSC and CISA advice set out below should help mitigate the risk to individuals and organisations from malicious cyber activity related to both COVID-19 and other themes:

- NCSC guidance for the public to help them spot, understand and deal with suspicious messages and emails: https://www.ncsc.gov.uk/guidance/suspicious-email-actions
- NCSC phishing guidance for organisations and cyber security professionals: https://www.ncsc.gov.uk/guidance/phishing
- NCSC guidance on mitigating malware and ransomware attacks: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
- NCSC guidance on home working: https://www.ncsc.gov.uk/guidance/home-working

[18] https://www.gov.uk/coronavirus
[19] https://www.gov.uk/government/organisations/public-health-england
[20] https://www.nhs.uk/conditions/coronavirus-covid-19/

- NCSC guidance on End User Device security: https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/vpns
- CISA guidance for defending against COVID-19 cyber scams: https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams
- CISA Insights: Risk Management for Novel Coronavirus (COVID-19), which provides guidance for executives regarding physical, supply chain, and cybersecurity issues related to COVID-19: https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf
- CISA Alert (AA20-073A) on enterprise VPN security: https://www.us-cert.gov/ncas/alerts/aa20-073a
- CISA website providing a repository of the agency's publicly available COVID-19 guidance: https://www.cisa.gov/coronavirus

Phishing guidance for individuals

The NCSC's suspicious email guidance explains what to do if you've already clicked on a potentially malicious email, attachment or link. It provides advice on who to contact if your account or device has been compromised and some of the mitigation steps you can take (such as changing your passwords). It also offers NCSC's top tips for spotting a phishing email:

- **Authority** - Is the sender claiming to be from someone official (like your bank, doctor, a solicitor, government department)? Criminals often pretend to be important people or organisations to trick you into doing what they want.
- **Urgency** - Are you told you have a limited time to respond (like in 24 hours or immediately)? Criminals often threaten you with fines or other negative consequences.
- **Emotion** - Does the message make you panic, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.
- **Scarcity** - Is the message offering something in short supply (like concert tickets, money or a cure for medical conditions)? Fear of missing out on a good deal or opportunity can make you respond quickly.

Phishing guidance for organisations and cyber security professionals

Organisational defences against phishing often rely exclusively on users being able to spot phishing emails. However, you should widen your defences to include more technical measures. This will improve your resilience against phishing attacks.

In addition to educating users on defending against these attacks, you should consider NCSC's guidance for organisations that splits the mitigations into four layers, on which you can build your defences:

1. Make it difficult for attackers to reach your users

2. Help users identify and report suspected phishing emails (see CISA Tips, Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams)
3. Protect your organisation from the effects of undetected phishing emails
4. Respond quickly to incidents

NCSC and CISA also recommend organisations plan for a percentage of phishing attacks to be successful. Planning for these incidents will help minimise the damage caused.

Communications platforms guidance for individuals and organisations

Due to COVID-19, an increasing number of organisations and individuals are turning to communications platforms (such as Zoom and Microsoft Teams) for online meetings. In turn, malicious cyber actors are hijacking online meetings that are not secured with passwords or that use unpatched software.

Tips for defending against online meeting hijacking (Source: FBI March 30, 2020 press release, *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic*):

- Do not make meetings public. Instead, require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to meeting on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screensharing options. Change screensharing to “Host Only.”
- Ensure users are using the updated version of remote access/meeting applications.
- Ensure telework policies address requirements for physical and information security.

Disclaimers

This report draws on information derived from NCSC, CISA and industry sources. Any findings and recommendations made have not been provided with the intention of avoiding all risks, and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favouring by CISA.