National Cyber Security Centre
a part of GCHQ

COVID-19 CYBER THREAT EXPLOITATION

The Threat and How to Think About It

The Cybersecurity and Infrastructure Security Agency (CISA) and United Kingdom's National Cyber Security Centre (NCSC) have seen an increase in malicious activity with themes related to Coronavirus Disease 2019 (COVID-19). Malicious cyber actors are targeting individuals, small and medium enterprises, and large organizations worldwide with COVID-19-related scams and phishing campaigns (see figure 1). At the same time, the surge in teleworking has increased the use of potentially vulnerable services.

Additionally, CISA and NCSC are investigating advanced persistent threat (APT) activity targeting healthcare and essential services. This activity includes password spraying—a commonly used style of brute force attack in which the attacker tries a single and commonly used password against many accounts before moving on to try a second password, and so on.

This product provides practical advice for individuals and organizations on how to defend against COVID-19-related malicious cyber activity.

For detailed guidance on these threats, see the CISA-NCSC joint Alert on COVID-19-related malicious cyber activity as well as the CISA-NCSC joint Alert on APT activity targeting healthcare and essential services.

Actions To Take Today

Communication Platform Guidance for Individuals and Organizations[1]

Limit screensharing options

Do not make meetings public.

Ensure users have the most up-to-date version of remote access/meeting applications

Do not share links to meetings on unrestricted, publicly available social media posts.

Ensure telework policies address requirements for physical and information security.

Guidance for Defending Against Password Spraying Attacks

Set up a security monitoring capability so you are collecting the data that will be needed to analyze network intrusions.

Use multi-factor authentication to reduce the impact of password compromises.

Review and refresh your incident management processes.

Protect the management interfaces of your critical systems. Use browse-down architecture to prevent attackers easily gaining privileged access.

Use modern systems and software. These have better security built-in.

[1] FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic, FBI press release, March 30, 2020, https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

Actions To Take Today Continued on next page >

Actions To Take Today - CONTINUED

Phishing Guidance for Organizations

Make it difficult for attackers to reach your users.

Help users identify and report suspected phishing emails.

Protect your organization from the effects of undetected phishing emails.

Plan for and respond quickly to phishing incidents.

Phishing Guidance for Individuals[1]

Use caution when opening email attachments from unsolicited emails or unknown senders.

Avoid clicking on links in unsolicited emails.

Do not respond to email solicitations for personal or financial information.

Learn how to recognize potential phishing emails. Refer to NCSC's suspicious email guidance for more information.

[1] For more information, see CISA Tip Avoiding Social Engineering and Phishing Scams.

Additional Resources

CISA is working with law enforcement and industry partners to disrupt or prevent malicious COVID-19-themed cyber activities. CISA and NCSC published a non-exhaustive list of COVID-19-related indicators of compromise (IOCs):

- CSV file
- STIX file

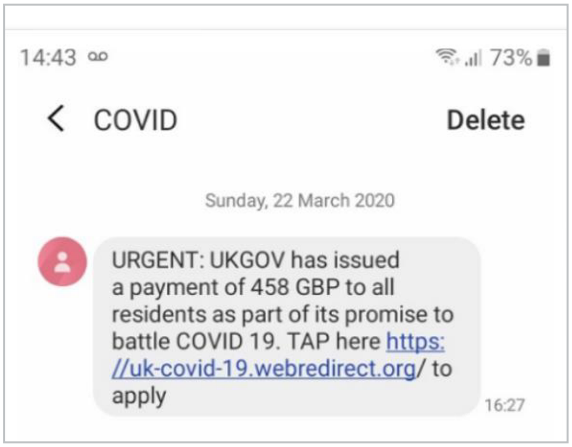
Review the following resources for additional guidance on decreasing cyber risks:

CISA Guidance

- Defending against COVID-19 cyber scams
- Risk Management for Novel Coronavirus (COVID-19)
- Enterprise VPN Security
- Cyber Essentials for small organizations
- Alert on password spraying attacks

NCSC Guidance

- Suspicious messages and emails
- Phishing for organizations and cybersecurity professionals
- Mitigating malware and ransomware attacks
- Cyber Aware guidance on staying secure online during coronavirus
- Guidance on defending against password spraying attacks



14:43 73%

COVID Delete

Sunday, 22 March 2020

URGENT: UKGOV has issued a payment of 458 GBP to all residents as part of its promise to battle COVID 19. TAP here https://uk-covid-19.webredirect.org/ to apply

16:27

Figure 1 . UK government-themed SMS phishing