CGI

Experience the commitment®

Cyber security Hygiene During COVID-19

A dos and don’ts guide to share with your employees

The Threat

It is an unfortunate fact that cyber threat actors will seize on adverse situations to achieve their goals. All security centres in government and industry are reporting a significant spike in malicious activities which exploit the current Coronavirus pandemic (COVID-19), feeding off people’s fears and uncertainties.

Many of these activities are taking the form of phishing attacks designed to look official but with malicious intent. Malicious emails and text messages can be spoofed (faked) to appear to come from legitimate and trustworthy sources.

Clicking on these links or an attachment can quickly infect unwary users with malware such as Worms, Trojans, Rootkits, Keyloggers, Ransomware and so on. Similarly, apps and ‘infection tracker maps’ can also be used to infect users' machines and phones.

TIPS FOR USERS

Many organisations are now requiring their staff to work from home, which can further increase the risk as enterprise network security safeguards are not always available to home-users, and some users may be forced to use their personal systems at home which may not have the same level of protection that end-points at work have.

Regardless of the circumstances you work under, we must all be especially vigilant right now for malicious attacks that attempt to exploit the pandemic and people's fears. This applies whether you are working in the office, or at home.

WATCH FOR THESE SIGNS

There are no foolproof methods to detect all attacks and this can be especially challenging for ordinary users. However, any one of the following contents should raise red flags:

- Unexpected or unsolicited emails – Be wary of any emails you receive on this subject that you were not expecting – even from friends (whose email address may have been captured from social media and spoofed), or supposedly authoritative agencies.
- Emails stressing urgency, especially those announcing new pandemic details and asking you to click on a link, or provide personal details to subscribe to announcements.
- Uses odd or unfamiliar greetings such as "Dear Sir/Madam."
- Uses odd email addresses that are out of place (or misspelt) for the agency portrayed. One actual case purported to come from a Federal agency but used an aol.com address.
- Spelling or grammar errors. Be suspicious of text phrased in an odd way.
- Contains attachments – As a rule, do NOT open attachments if you were not expecting them. If in doubt and the sender is a friend or colleague, check with them first to verify before opening it.
- Embedded links – Be wary of them. You can hover your mouse over the link to see if the 'advertised' address matches the link provided. Still, the safest option is to navigate independently to the official website of the agency quoted and not use the link in the email. Even if you do click on a malicious link, do not feel reassured if you receive a notice such as "404 ERROR – WEBSITE NOT FOUND." You may still have been compromised.

WORKING FROM HOME

Many people are now being asked to work from home, which can introduce additional risks, as explained above. Here are some 'hygiene' tips to help reduce these risks:

- Wherever possible only use a laptop issued by your work – It likely contains more robust security safeguards than your personal computer.
- Where available use an approved secure remote access connection to connect to work – Most such connections include an encrypted point-to-point VPN session.
- Ensure your end-point is updated – Ensure that all available software and security updates and patches have been applied and that your anti-malware is up to date and has the latest DAT files.
- Do not disable security safeguards such as anti-malware or end-point firewalls.
- Do not browse the web while not connected to your corporate VPN. While connected, you will likely benefit from additional protections in your enterprise network.
- Unattended computers – If you have to leave your computer unattended, ensure that you close any remote access connection and either lock your screen with a password or shut it down.
- Avoid using public Wi-Fi or conducting work in public places.
- Consider your surroundings – While working from home, family members or housemates may overhear conversations or see documentation related to your work which they shouldn't have access to. Follow existing policy on the need to know and clear desks.
- Keep in touch with your organisation and stay alert for any announcements about cyber security.

USE TRUSTED SITES

In addition to malicious threats, many internet sites are spreading erroneous or misleading information regarding COVID-19. Therefore, we strongly recommended that you only rely on information from the following authoritative agencies and that you navigate directly to these sites in your browser:

- World Health Organisation - https://www.who.int
- UK Government - https://www.gov.uk/coronavirus
- UK Health Authority - https://www.nhs.uk
- National Cyber Security Centre - https://www.ncsc.gov.uk

SIGNS OF COMPROMISE

Depending on the skill of the attacker, you may not see indications of compromise. However, in some cases, you may, and the following are the common symptoms:

- Pop-up windows appearing on your system when there were none previously
- Your browser's homepage changes
- Unexpected system and application behaviour, including page, application and/or system crashes
- Slow computer performance
- Unknown programs running on your system
- Anti-Malware software becomes disabled
- Unauthorised password changes or unexpected requests for password changes/validation

IMMEDIATE ACTIONS IF COMPROMISED

If you have reason to suspect your computer may be compromised, take the following actions immediately:

- Terminate any remote access sessions
- Disconnect your computer from all wired and Wi-Fi connections
- Where organisational policy allows, power-off your computer
- Contact your organisation's security service desk and follow their instructions

CONCLUSION

The cyber security threat, especially for those working from home, is yet another dimension of the current COVID-19 pandemic. However, you can reduce the threat by being aware of and following the guidelines above. For additional information related to the COVID-19 cyber security threat, please navigate directly to the official National Cyber Security Centre website.

For any questions around cyber security reach out to **enquiry.uk@cgi.com**.