National Cyber Security Centre

2004011554-NCSC

A part of **Department of Communications, Climate Action & Environment**

NCSC Advisory

Working From Home Security Advice
2020-04-08

Status: TLP-WHITE

NCSC

Traffic Light Protocol

This document is classified using Traffic Light Protocol. Recipients may share TLP: WHITE information freely, without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. **Please treat this document in accordance with the TLP assigned.**

Working From Home - Threats

The recent COVID-19 situation has suddenly presented IT personnel and users with a set of cyber security challenges that, whilst not unique, are being experienced on a significantly larger scale than ever before. In that context the NCSC has created this document to provide advice on how to secure your home office against cyber-related threats.

Criminals exploiting tragedies and events for their own profit is not new to security specialists. However, the speed and scale at which cyber criminals and state actors have adapted their operations to exploit the general public's anxiety and vulnerabilities created by the response to the COVID-19 pandemic has created a considerable amount of concern amongst the cyber security community.

These adaptations include:

- Reusing existing infrastructure with COVID-19-themed lures and texts
- Creating additional infrastructure to mimic COVID-19 related organisations
- Targeting organisations staff that are working from home
- Targeting health care services that are under stress with responding to COVID-19
- Exploiting weaknesses introduced into business processes from their response to COVID-19
- Creating malware with COVID-19 themes

The key threats to organisations during the response to COVID-19 stem from the Phishing, Social Engineering and Remote Access Threat. These are not new threats, but with large numbers of staff working from home, there may be additional vulnerabilities where existing IT security services do not extend to remote devices, and where remote working was implemented under time pressure.

Phishing

Email is a common attack vector for such crimes with over 90% of cyber attacks beginning with an email [1]. In addition to the regular email phishing; phones are also targeted through SMS phishing (smishing) and through malicious links embedded in popular messaging & social media apps. Criminals have adapted their phishing lures to reference the pandemic directly, pretending to be documents or information from relevant national or international public health authorities. They have also created infrastructure to mimic those institutions and other healthcare services, for example, tens of thousand of domains with deceptive names have been registered.

[1] https://pages.checkpoint.com/phishing-attacks-put-your-business-at-risk.html

The ultimate goal of this activity remains the same as before: stealing credentials for access or resale, installing malware to damage infrastructure or allow remote access.

"Cofense", a phishing prevention and mitigating firm reported that it has not seen an increase in the volume of emails that get through the infrastructure protections: email gateways and email scanners. It does note that 80% of those that have, have changed to COVID-19 lures.[2]

Please consider the following when processing emails in the current climate:

- Many phishing emails have poor grammar, punctuation and spelling
- Ensure employees are aware of this type of threat and how to avoid it
- Always check email addresses carefully, particularly if there is any financial implications to requested actions
- Please be wary of any emails referencing Coronavirus from an unrecognised source
- Criminals will use the fear and uncertainty surrounding Coronavirus to scam users
- Manually type in URLs to sites you want to visit rather than clicking on links
- Verify the mail - Do not contact the supplier of the invoice through links or the phone number supplied within the mail. Do not reply directly to the email. Contact a known supplier through pre-existing channels

Vishing

Please be wary of unsolicited phone calls claiming to be from banks, internet providers or any other entity requesting passwords, usernames or money for any service. If necessary contact the site or service through an established contact method and not through any links or numbers provided within the communication received. In addition NCSC has been notified by international partners of Vishing calls aimed at remote workers pretending to be from their parent organisation's IT department asking them for credentials or to attempt to fool the user into installing malware by pretending to run diagnostics or peform maintenance on their home laptop. These threats are evident in other countries and its highly likely that such occurrences will be observed in Ireland as the COVID-19 situation continues to evolve.

Social Engineering & Business Email Compromise (BEC)

In normal operations, organisations may have processes and standards to permit remote working for staff. These processes may include a health and safety survey on the users proposed workspace, a formal approval process, an evaluation on personal devices used for work purposes, and other

[2] https://cofense.com/category/threat-intelligence/

specialised tests to ensure business continuity. All these processes and communications can be opportunities for criminal social engineers to deceive staff by pretending to be a debtor, creditor, senior management or IT administrator in order to send emails attempting to elicit some form of payment or sensitive information from unsuspecting employees. These operations may result in electronic funds transfer from the orgnaisation to criminal-run accounts, know as invoice fraud, or passwords, bank details and other credentials being inadvertently passed to criminal actors pretending to be an associate or employee of an organisation.

A BEC group named "Ancient Tortoise" [3] started using COVID-19 lures as far back as February. In its previous operations, this group convinced staff to release the organisations list of overdue accounts, who were in turn then pressured for payments to accounts controlled by criminals. More generally, criminals may ask for an organisation to change a creditor's bank details to an account controlled by the criminal, this invoice redirection fraud may be done on pretext of a COVID-19 response. Also, staff may get an urgent message from senior management requesting a payment to an account in order to help the organisation respond to COVID-19 restrictions.

People should be wary of BEC and enhanced vigilance should be practiced when receiving emails from vendors/clients notifying of a change of bank account and requesting payments made into the new account. Users should verify the change using established forms of communication and not through contact details within the suspicious email. If in doubt make a phone call to confirm the request.

Remote Access Threat

Similarly, the threat from Remote Access Trojans (RATs) is not new. Large numbers of staff working remotely create more opportunities to exploit vulnerabilities in a more widespread fashion. Criminals may extend their attempts to brute force VPN credentials in order to gain access to the corporate network. They can also attack home routers to gain access to the main WAN on a much larger scale. Many home routers use a default password and have other security issues (See: Home Router Hardening) or the attacker may simply decide to send an email with a malicious link or attachment to deliver the malicious payload.

Once unauthorised access has been gained a RAT (Remote Access Trojan) is deployed on the victim machine. Attackers now have remote control of the compromised device. Instances of NanoCore RAT[4], Remcos RAT [5] and Lime RAT [6] have all been observed by NCSC in recent weeks with the initial delivery vector associated with some form of COVID-19 related theme. These RATs can then be instructed by the remote attacker to identify valuable data and exfiltrate for the purposes of further exploitation.

[3] https://www.agari.com/email-security-blog/ancient-tortoise-bec-attack-chain/
[4] https://attack.mitre.org/software/S0336/
[5] https://attack.mitre.org/software/S0332/
[6] https://malpedia.caad.fkie.fraunhofer.de/details/win.limerat

Keeping Your Home Work Environment Cyber Secure

Secure Password Policy

This next section is a standing section in almost all NCSC documentation. It's a standing section because the incident response team still witnesses both in Ireland and globally, major security breaches every year due to poor password management. NCSC's simple message is **"Read and Heed!"**.

NCSC Password Advice

- Passwords should be at least 12 characters in length
  - Consider using passphrases; these are easier to remember and help in creating longer, more complex passwords
  - Use random and unrelated words. The greater the complexity
  - Use words that do not appear in the dictionary
  - Use words from different languages
  - Use a combination of random numerical and special characters throughout the passphrase
  - Do not use common phrases or quotes
  - Do not use personal words like family names, pets, local football club or anything associated with your personal life
  - Do not use words or abbreviations associated with your organisation or industry
- Enable Multi-Factor Authentication (MFA). Multi-Factor Authentication, also known as MFA or 2FA involves using your username and password and one other piece of information. This other piece of information can come in various forms. It may be:
  - A one time dynamically issued token
  - A physical object in the possession of the user
  - A physical characteristic of the user (biometrics)
  - An additional piece of information that is only known to the user
- Consider using Password managers as an easy way to manage multiple complex passwords[a]
- Do not reuse passwords across multiple accounts
- Reiterate to users the importance of secure password hygiene, not just with their work accounts but also with their personal accounts

[a] https://www.wired.com/story/best-password-managers/

Home Router Hardening - 5 Simple Tips

Here are five simple tips to help the home worker ensure their home WiFi affords them a little more protection from malicious cyber activity.

Hide home wireless network SSID name: This step will prevent your network name from being seen by those in proximity to your home router. It prevents your network appearing on “available networks list” of any device within range of your home wireless router. Hiding your SSID does not prevent your home WiFi network from detection, as your SSID is still visible using a simple WiFi scanning tool, but if an opportunistic attacker were in the vicinity they are more likely to choose a non-hidden SSID.

Change your wireless network SSID name: ISPs provide routers to customers with a default SSID name and password. The default name is chosen by the manufactures of the routers, with many manufacturers having their own particular naming convention. Whilst not a security issue in itself, revealing your SSID default name will facilitate nefarious actors identifying the make and model of your home router and thereby allowing them to potentially determine if a vulnerability exists for that particular device. When renaming your router never use an SSID name that might give away the identity of your home or family.

Disable WPS (Wi-Fi Protected Setup): This feature was found to have a vulnerability a number of years ago but still remains enabled by default on many routers. Aimed at providing a simplified mechanism for setting up WiFi networks, the PIN authentication method for WPS can be easily brute-forced thereby granting access to an attacker.

Turn off Guest Networking: In certain circumstances home routers have a Guest access feature enabled by default. This obviates the need for a security key when accessing a WiFi network. NCSC advises that if the Guest access is enabled you disable this option in your router settings.

Choose Strong Security Protocol: Ensure you select “WPA2” or the newer “WPA3” for your router’s WiFi security protocol, and make sure your password is hard to guess (see "Secure Password Policy") . Consider using a wired connection (Ethernet/RJ45 cable) to connect to your router if possible.

Remote Conferencing

As remote working becomes part of our day-to-day lives, the use of remote conferencing technologies such as Zoom, WebEx, MS Teams have grown in a sudden and not always structured manner. Conference calls are by their nature an open and not always secure environment by virtue of the fact you are never entirely sure of whom you are speaking to particularly in larger meetings. Discussions of a confidential or classified nature should not be conducted over these means and due care and attention should be taken when it comes to the management of remote video conferences (identity verification, PIN access). Given the difficulties in ensuring a fully secure multi-party video conference in general, a good rule of thumb is: **"Assume what goes on a Video Conference will not always stay on a Video Conference."**

Advice for Hosting Securing Remote Conferences

The NCSC offers the following advice for securing virtual meetings:

- Keep the application updated at all times
- Prioritise using the Web Browser over Desktop or mobile application to access your web conferencing application
- Enable Multi-Factor Authentication (MFA) on your Web-Conferencing account
- Use a password or PIN function where available to enter meetings and only share it with those scheduled to attend the meeting
- Send passwords or PIN via out-of-band means e.g. text or Signal message. Use of the meeting ID function is preferable to sharing a link
- When scheduling a meeting avail of "Waiting Room" or "Green Room" function
- Make sure to enable features that alert of newly joined participants - audible tone
- The host should restrict who is allowed to use their camera and microphone
- Minimise the use of the chat and file sharing functions or disable entirely if not required
- Do not give control of your screen unless you know and can verify the individual you are passing control (Present in same room)
- Select "Lock Meeting" function or similar once all expected guests have joined the meeting
- Before starting a meeting, make sure to check who exactly is on the call from the Participants menu
- Consider making registration a requirement
- Do not record meetings unless it is strictly necessary

Use of Work-Issued Devices

When working at home it is important to remember your device and access to your work systems or data is authorised for staff use only. Care should be taken to protect work-issued equipment both from inadvertent or deliberate unauthorised access. To assist with this process the NCSC has provided the following advice:

Keeping Work Devices Safe

- Work-issued devices(such as desktops, laptops, mobile phones or tablets) must not be used by anyone other than you. Family members or housemates must not be given access to such devices.
- Do not encourage children to access your orginisational devices by putting games or playing videos to occupy them for short periods. Work devices or devices being used to access orginisational resources should always be off limits.
- Please handle hard copy documents and printouts carefully. Do not place confidential material that would normally be shredded in the office in your recycle bin when working from home (even if children have coloured on it!). Avoid printing material outside of the office but if you must, please ensure that you store and handle the documents in line with the sensitivity of the material they contain.
- Avoid using shared family electronic resources for the storage or processing of work data. These types of shared facilities can greatly increase the risk of compromise to the security of the data, undermine the integrity and management of that data and lead to your personal devices being in scope for any subsequent follow-on actions, including legal or FOI. Remember access to corporate data and systems has been granted to staff and using shared resources can allow access to people who have not been authorised for that access.
- Be careful of where you store and use your corporate electronic equipment or hard copies of documents so as to avoid loss, damage or theft. Always keep them in a secure location. e.g. don't leave them on view in the passenger compartment of your car.
- All devices must require password or PIN to unlock/login.
- Do not write down or share your passwords, tokens, usernames etc.
- Never leave sensitive information unencrypted at home or in public spaces.
- All devices must have a short inactivity timeout such that they lock automatically after a short period of non-use.
- When leaving any such device unattended, you must ensure the device is locked (i.e. returned to login/PIN to unlock screen)
- Be aware that your device may have an IT policy applied that results in the device being completely wiped (factory reset) if the password/PIN is entered a certain number of times incorrectly.
- At the end of each day desktops/laptops should be powered off.

Be mindful of the "Physical security" of your organisation's equipment and data entrusted to you.

Use of Personal Devices For Work Purposes

If using a personal device to access, process or store work-related data, such devices should ideally follow the same guidelines as those outlined in “Use of Work-Issued Devices” Where a device is a shared device, the following security precautions should be taken.

Advice for Securing Personal Shared Devices

- A separate login should be created for your exclusive use on such devices where practicable
- Logins/PINs and inactivity restrictions should apply to that Login as per “Use of Work Provided Devices”
- Saving sensitive data to a shared device should be avoided
- Where a separate login cannot be created, access to work related systems and data must only be conducted through the use of self-contained or “containerised” applications where login/PIN and inactivity controls can be applied to the application in use rather than the device as a whole

If in doubt about any of these recommendations consult your IT department as they may have more specific guidelines for your particular work needs. Familiarise yourself with your IT department’s policies for remote working and use of mobile devices.

Feedback and Reporting

NCSC-IE wishes to offer whatever assistance it can in relation to this current situation and is willing to work with the relevant parties to further understand the current threat. NCSC-IE would also request any feedback in relation to this advisory as regards the relevance and accuracy of the information provided. For further details on how to report a cyber security incident to the NCSC please see the https://www.ncsc.gov.ie

Cyber security vs Cyber crime

There are a number of cyber-related events which may not be considered as cyber security incidents but could constitute a cyber crime. Cyber bullying, threats via email, text or instant message, online fraud or online extortion are all examples of potential cyber crimes. If you feel you have been a victim of a cybercrime you should contact An Garda Síochána.

If you wish to learn more about staying safe online please visit https://www.gov.ie/en/campaigns/be-safe-online/, a Government campaign aimed at highlighting ways to help people stay safe whilst conducting online activites.

If you are experiencing unexpected or unusual network issues it is recommended that you contact your system administrator or service provider to identify the root cause of the issue before reporting the issue to this office.

How to report a Governmental security incident

If you believe that you are experiencing a cyber security incident that is of national concern and wish to notify us directly you can email NCSC at info@ncsc.gov.ie. If you wish to report a security incident and you are an agent of one of NCSC's constituents (e.g. an official in a government department with the authority to make such a report) please email incident@ncsc.gov.ie or certreport@dccae.gov.ie