EXCELLIUM

Your first call when it comes to IT and security

COVID-19 threats and recommendations

Monday April, 6th 2020

Table of Contents

Foreword

Today is April 6th. The COVID-19 pandemic is raging around the globe. 1.275 million confirmed cases have been registered, 70 000 people have died.

And of course, hackers are not going to take a break… On the contrary, hackers are jumping on the pandemic to try to use it for their own gain.

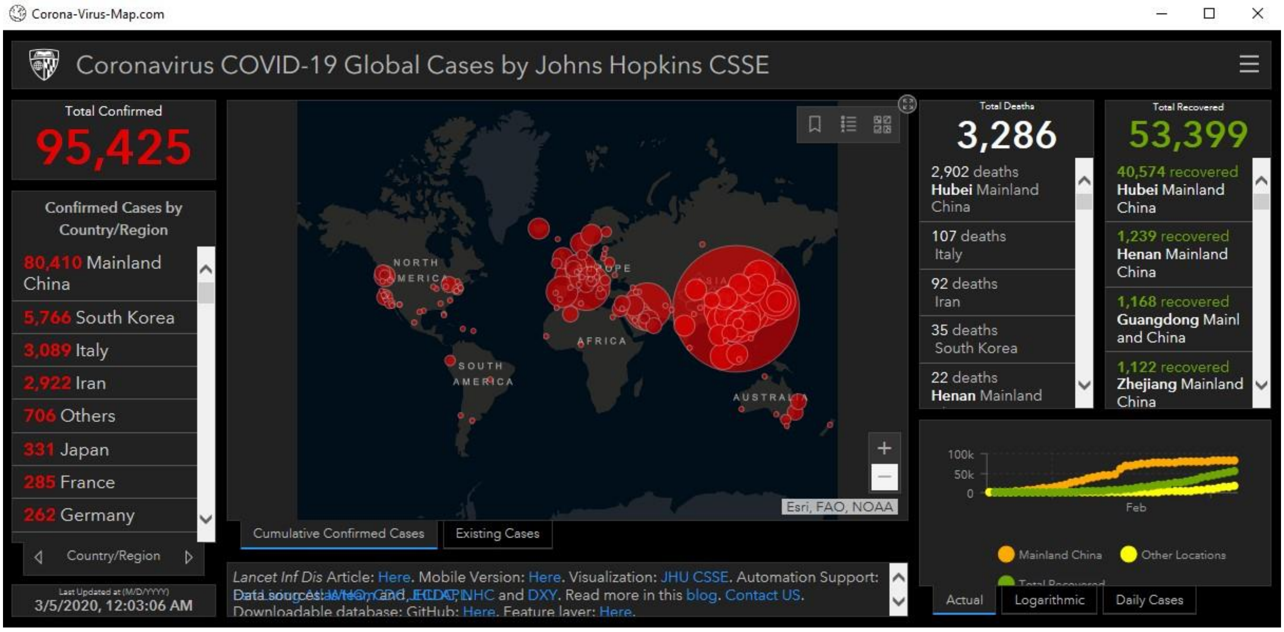
1. A growing number of scams exploiting COVID-19

According to a report published by Check Point Research[1], hackers are exploiting the COVID-19 outbreak to spread their own infection, including registering malicious Coronavirus-related domains and selling malware on the dark web.

These are just a few of many COVID-19 related cyberattacks i.e against hospitals[2], phishing campaigns that distribute malware such as AZORult[3], Emotet[4], Nanocore RAT[5] and TrickBot[6] via malicious links and attachments[7], and execute malware and ransomware attacks that aim to profit off the global health concern.

1.1. Scam example #1: Info-Stealing Coronavirus Threat Map

Researchers have found[8] that cybercriminals are running a fake coronavirus threat map website to steal personal information. Victims who visit the page are shown a map of the globe highlighting to which countries the virus has spread together with stats on the number of deaths and infections recorded. To give the fake and malicious map an extra authenticity, criminals have designed it to mimic a legitimate COVID-19 threat map created by Johns Hopkins University that similarly shows countries hit by the virus together with the latest statistics.



Corona-Virus-Map.com

Coronavirus COVID-19 Global Cases by Johns Hopkins CSSE

Total Confirmed
95,425

Confirmed Cases by Country/Region

80,410	Mainland China
5,766	South Korea
3,089	Italy
2,922	Iran
706	Others
331	Japan
285	France
262	Germany

Last Updated at (M/D/YYYY)
3/5/2020, 12:03:06 AM

Total Deaths
3,286

2,902 deaths Hubei Mainland China
107 deaths Italy
92 deaths Iran
35 deaths South Korea
22 deaths Henan Mainland

Total Recovered
53,399

40,574 recovered Hubei Mainland China
1,239 recovered Henan Mainland China
1,168 recovered Guangdong Mainland China
1,122 recovered Zhejiang Mainland China

Lancet Inf Dis Article: Here. Mobile Version: Here. Visualization: JHU CSSE. Automation Support: Data sources: WHO, CDC, ECDC, NHC and DXY. Read more in this blog. Contact US.
Downloadable database: GitHub: Here. Feature layer: Here.

Emails containing links to the fake map were discovered. Victims who clicked on the links unknowingly activated malicious information-stealing software. The malware can be used to steal browsing history, cookies, ID/ passwords,

[1] https://blog.checkpoint.com/2020/03/19/covid-19-impact-as-retailers-close-their-doors-hackers-open-for-business/

[2] https://www.reuters.com/article/us-healthcare-coronavirus-usa-cyberattac/cyberattack-hits-u-s-health-department-amidcoronavirus-crisis-idUSKBN21320V

[3] https://www.proofpoint.com/us/corporate-blog/post/attackers-expand-coronavirus-themed-attacks-and-prey-conspiracytheories

[4] https://blog.checkpoint.com/2020/02/13/january-2020s-most-wanted-malware-coronavirus-themed-spam-spreads-maliciousemotet-malware/

[5] https://blog.talosintelligence.com/2020/02/coronavirus-themed-malware.html

[6] https://nakedsecurity.sophos.com/2020/03/05/coronavirus-warning-spreads-computer-virus/

[7] https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/multiple-phishing-attacks-discovered-using-thecoronavirus-theme/

[8] https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/

cryptocurrency, credit card information stored in users' browser history, and more. It can also download additional malicious software onto infected machines.

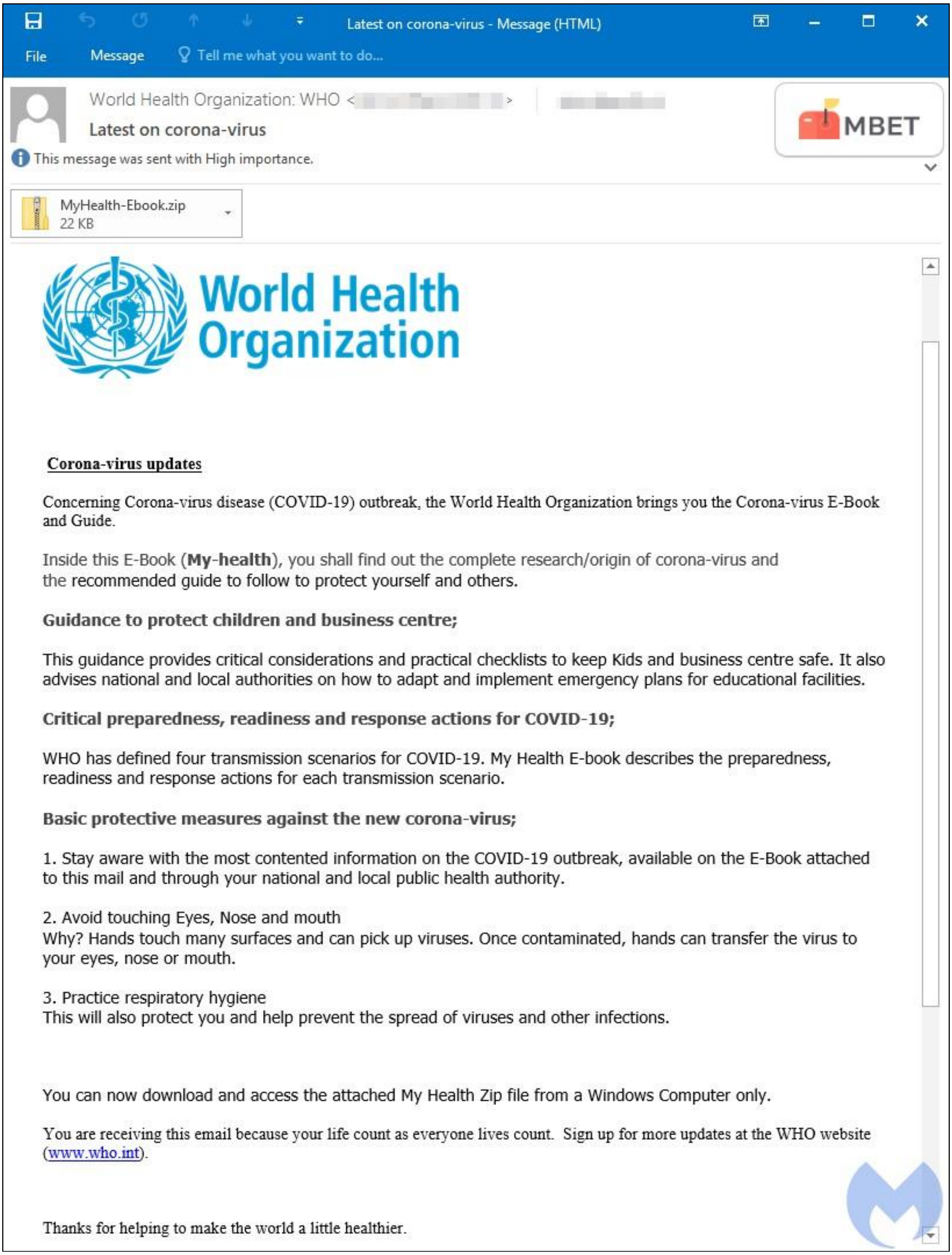
1.2. Scam example #2: Coronavirus Phishing Scams

In the past week, security researchers have discovered multiple email scams that prey on the fear, uncertainty, and confusion regarding COVID-19. With no vaccine yet developed, and with much of the world undergoing intense social distancing measures and near-total lockdown procedures, threat actors are flooding cyberspace with emailed promises of health tips, protective diets, and, most dangerously, cures.

Attached to threat actors’ emails are a variety of fraudulent e-books, informational packets, and missed invoices that hide a series of keyloggers, ransomware, and data stealers.

For example, security researchers[9] reported this phishing campaign which impersonates the World Health Organization (WHO) and promises the latest on “corona-virus.”. You can notice right away the incorrect use of a hyphen in “coronavirus” in the subject line. However, since WHO are often touted as a trustworthy and authoritative resource, many will be tempted to open the email.

[9] https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-todistribute-fake-coronavirus-e-book/


Latest on corona-virus - Message (HTML)
File
Message
Tell me what you want to do...
MBET
World Health Organization

World Health Organization: WHO <[redacted]> [redacted]

Latest on corona-virus

This message was sent with High importance.

MyHealth-Ebook.zip
22 KB

Corona-virus updates

Concerning Corona-virus disease (COVID-19) outbreak, the World Health Organization brings you the Corona-virus E-Book and Guide.

Inside this E-Book (**My-health**), you shall find out the complete research/origin of corona-virus and the recommended guide to follow to protect yourself and others.

Guidance to protect children and business centre;

This guidance provides critical considerations and practical checklists to keep Kids and business centre safe. It also advises national and local authorities on how to adapt and implement emergency plans for educational facilities.

Critical preparedness, readiness and response actions for COVID-19;

WHO has defined four transmission scenarios for COVID-19. My Health E-book describes the preparedness, readiness and response actions for each transmission scenario.

Basic protective measures against the new corona-virus;

1. Stay aware with the most contented information on the COVID-19 outbreak, available on the E-Book attached to this mail and through your national and local public health authority.

2. Avoid touching Eyes, Nose and mouth
Why? Hands touch many surfaces and can pick up viruses. Once contaminated, hands can transfer the virus to your eyes, nose or mouth.

3. Practice respiratory hygiene
This will also protect you and help prevent the spread of viruses and other infections.

You can now download and access the attached My Health Zip file from a Windows Computer only.

You are receiving this email because your life count as everyone lives count. Sign up for more updates at the WHO website (www.who.int).

Thanks for helping to make the world a little healthier.

In this particular campaign, threat actors use a fake e-book as a lure, claiming the “My Health E-book” includes complete research on the global pandemic, as well as guidance on how to protect children and businesses.

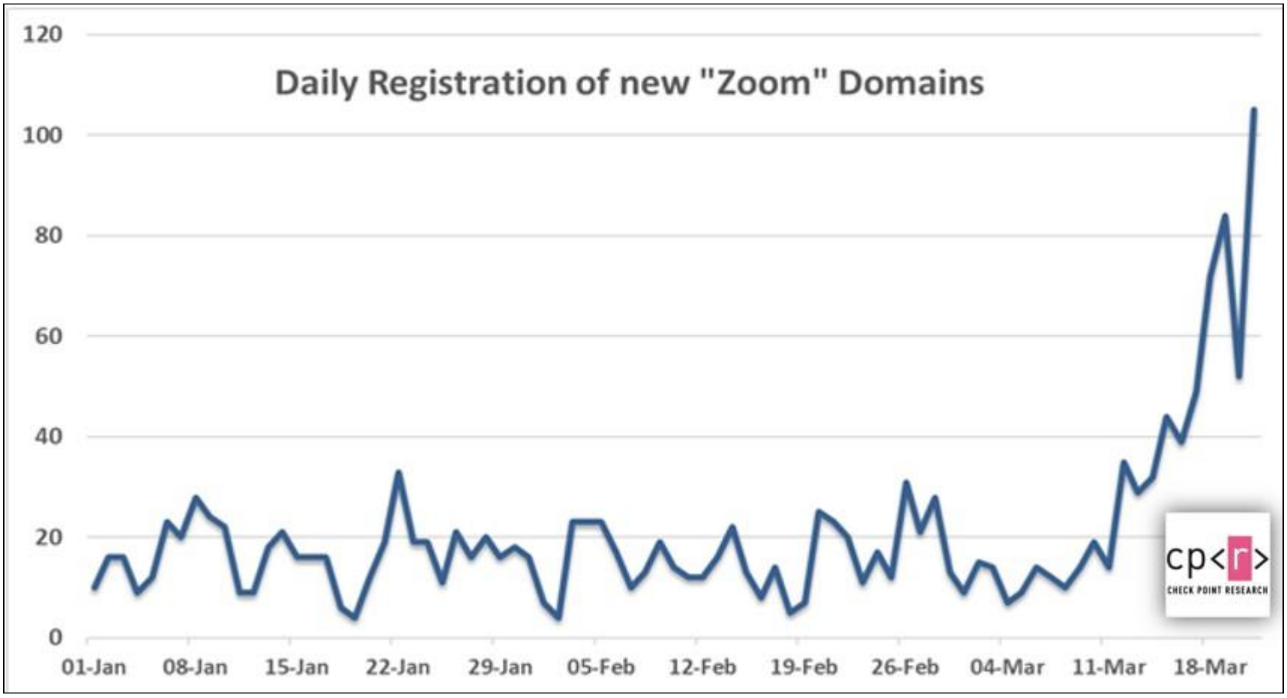
The criminals behind this scheme try to trick victims into opening the attachment, contained in a zip file, by offering teaser content within the body of the email.

As soon as the victims open the file inside the MyHealth-Ebook.zip archive, malware will be downloaded onto their computers.

1.3. Scam example #3: Exploiting Zoom's Success to Spread Malware

As people increasingly work from home and online communication platforms such as Zoom explode in popularity in the wake of coronavirus outbreak, cybercriminals are taking advantage of the spike in usage by registering new fake "Zoom" domains and malicious "Zoom" executable files in an attempt to trick people into downloading malware on their devices.

According to a report published by Check Point[10], over 1,700 new "Zoom" domains have been registered since the onset of the pandemic, with 25 percent of the domains registered in the past seven days alone.



The researchers have detected malicious files with names such as “zoom-us-zoom_##########.exe” and “microsoft-teams_V#mu#D_##########.exe” (# representing various digits). The running of these files ultimately leads to malicious software installation.

[10] https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/

2. How to protect your organization?

Working from home can be new to some organizations, and even perhaps overwhelming to some employees. Since the number of people working remotely has increased dramatically, it is of vital importance to ensure an adequate level of cybersecurity when teleworking.

2.1. Recommendations for organizations

- Do not expose unnecessary or unsecured equipment, applications and services on the Internet (e.g MS Exchange web interfaces, SMB file sharing services, RDP, …); Pay particular attention to services that might have been exposed “in a rush” as an immediate action to the confinement
- Apply security fixes as soon as possible, especially for equipment, applications and services exposed on the Internet
- Make regular backups of your critical systems
- Ensure that all the corporate business applications are accessible only via encrypted communication channels e.g a corporate VPN solution
- Apply 2FA (Two Factor Authentication) or MFA (Multi Factor Authentication) mechanisms on equipment, applications and services exposed on the Internet (including for VPN access) in order to limit the risk of identity theft
- Provide secure video conferencing for corporate clients (both audio/video capabilities).
- Provide secured (e.g anti malware, disk encryption, …) and up-to-date corporate computers/devices to your staff while on teleworking
- Forbid the use of BYOD
- Ensure a proper information security awareness communication and training to your staff
- Regularly review the security logs of the systems exposed on the internet; Detect and respond to any suspicious behavior
- Ensure that your IT resources are in place to support staff in case of technical issues while teleworking; provide relevant information, e.g. on contact points, to staff.
- Ensure policies for responding to security incidents and personal data breaches are in place and that staff is appropriately informed of them.
- Ensure that any processing of staff data by the employer in the context of teleworking (e.g. time keeping) is in compliance with the EU legal framework on data protection.

2.2. Recommendations for employees

- Only use corporate laptops/phones/… Do not mix personal and professional activities on the same devices.
- Connect to the internet via secure networks like your home wifi. Avoid open/free networks (airport, hotel, public places, …)
- Ensure your VPN is enabled at all times
- Apply system (operating system and applications used, as well as anti-virus system) updates immediately
- Do not leave your laptop unintended unless you have locked your screen
- Do not share virtual meeting URLs on social media or other public channels
- On the use of emails:
    - Be particularly careful with any emails referencing the coronavirus, as these may be phishing attempts or scams
    - Be very suspicious of mails from people you don't know- especially if they ask to connect to links or open files
    - Mails that create an image of urgency or severe consequences are key candidates for phishing - in these cases always verify via an external channel before complying

- Mails sent from people you know, but asking for unusual things are also suspect - verify by phone if possible
- Any doubt, call your designated security contact

3. A word on Zoom and other audio/video conferencing platforms

Over the past few weeks in a COVID-19 world, audio/video conferencing platforms have become increasingly popular. Among them is the well-known Zoom service, which has now become infamous for its security and privacy concerns.

3.1. The Zoom controversy

Regarding Privacy, even though the company is somewhat working on "fixing privacy issues", it was and is still collecting a long list of data (for its own profit)[11] about you including user name, physical address, email address, phone number, job information, Facebook profile information, computer or phone specs, IP address, and any other information you create or upload. On top of that, Zoom is using third-party trackers and surveillance based advertising[12].

Regarding Security, several issues were raised, for example:

- Last year, a researcher discovered[13] that a vulnerability in the Mac Zoom client allowed any malicious website to bypass browser security settings and remotely enable a user's web camera without the user's knowledge or consent. Zoom patched this vulnerability last year.
- On April 1st, it was discovered that for Windows can be used to steal[14] users' Window credentials
- On April 2nd, we learned that Zoom secretly displayed data from people's LinkedIn profiles, which allowed some meeting participants to snoop on each other. Zoom has fixed this one since then.

At this stage, it is highly probably that there are a lot more security design shortcomings and software vulnerabilities coming.

However, to make things worse, Zoom encryption is certainly not state of the art:

- Zoom doesn't offer end-to-end encryption[15], but only provides link encryption. Everything is unencrypted on the company's servers.
- For each Zoom meeting, a single AES-128 key is used in ECB mode[16] by all participants to encrypt and decrypt audio and video. The use of ECB mode is not recommended because patterns present in the plaintext are preserved during encryption.

Zoom has a lot of configuration options. You certainly don't want to stick with the defaults. Otherwise, you may encounter such things as "Zoombombing"[17]: Because meeting IDs are too short to prevent someone from randomly trying them, some people are simply looking for open Zoom meetings, join them, and disrupt them somehow e.g sharing their screens to everyone with offensive content.

[11] https://www.schneier.com/blog/archives/2020/04/security_and_pr_1.html

[12] https://blogs.harvard.edu/doc/2020/03/30/zooms-new-privacy-policy/

[13] https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-yourwebsite-ac75c83f4ef5

[14] https://arstechnica.com/information-technology/2020/04/unpatched-zoom-bug-lets-attackers-steal-windows-credentialswith-no-warning/

[15] https://theintercept.com/2020/03/31/zoom-meeting-encryption/

[16] https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/

[17] https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html

3.2. Zoom: the best practices

The absolute best practice is to NOT use Zoom at all. But if for some reasons you are still going to, apply the following best practices:

- don't share the meeting IDs more than you have to
- use a password in addition to a meeting ID
- use the waiting room
- pay attention to who has what permissions
- user awareness: download Zoom clients from legitimate sources (MS Store or vendor web site), keep Zoom clients up-to-date, make sure to use the genuine domain name in URLs (https:// <your_company>.zoom.us[18])

3.3. Alternatives to Zoom

Please note that the following solutions are just an FYI. They have not been reviewed by Excellium Services. They may or may not be a drop-in replacement for Zoom. Make sure to properly assess them before implementing them in your organization.

3.3.1. CISCO Webex

Webex[19] is a videoconferencing app that was created in the '90s and was acquired by Cisco in 2007. It is commonly used as a business application and continues to focus on serving companies. A free version exists with extended features for the current emergency: up to 100 participants, unlimited timing for each meeting, call-in for audio.

3.3.2. Microsoft Teams

Microsoft Teams[20] is the video meeting choice for businesses using Office 365. It "enforces team-wide and organization-wide two-factor authentication, single sign-on through Active Directory, and encryption of data in transit and at rest," according to Microsoft.

3.3.3. Skype

Skype[21] is a nearly as functional as Zoom. It's stable, supports large group chats, doesn't require an account, and it's easy to create your own meeting and control who's allowed in. One important thing though: Skype isn't end-to-end encrypted.

3.3.4. Jitsi

Jitsi[22] is a secure open source app that offers multiple video chatting features, and people joining your chat don't have to create an account. All information that leaves your device is encrypted but again, it's not end-to-end encrypted. But since it's open source, you can host your own server to mitigate the risks. Jitsi is still somewhat new on the market, and can be a little jittery with multiple people joining the chat.

[18] http://zoom.us
[19] https://www.webex.com/
[20] https://products.office.com/en-gb/microsoft-teams/group-chat-software
[21] https://www.skype.com/en/
[22] https://jitsi.org/