ISEA
Information Security
Education & Awareness
www.isea.gov.in

For more details visit :
www.
InfoSec
awareness.in

Secure Remote Desktop Access

Advisory during the COVID-19 outbreak

Programme by : Ministry of Electronics & Information Technology(MeitY), Govt. of India

Supported by : Ministry of Home Affairs (MHA), Govt. of India

For Virus Alerts,Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents
http://cert-in.org.in/

www.
cyberswachhtakendra.
gov.in

CYBER DOST

Cyber Safe GIRL
Beti Bachao, Cyber Crime Se...

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

For more details / queries on
Cyber Security
Call us on our Toll free No.
1800 425 6235

Implemented by
सी डैक
CDAC

Information Security Education and Awareness (ISEA) Project Phase-II

Programme by
Ministry of Electronics and Information Technology
Government of India

Index:

Preface

The Coronavirus Disease or the COVID-19 pandemic is now a grave crisis that people across the world are facing. With no cure sighted, it is only the precautionary measures taken by common people that can keep it at bay; the major among these measures being social distancing or keeping away from crowds, gatherings and from each other to stop it from spreading further . Following the suit of social distancing many organizations across the world have been obliged to provide the option of work from home to its employees.

As working from home becomes mandatory due to COVID-19 pandemic, it is to be ensured that any endpoint that an employee uses is fully protected. Cybercriminals have started to exploit fears around the COVID-19 outbreak to conduct email scams, phishing and ransomware attacks. As per the Check Point research, there are 4,000 COVID-19 domains that have been registered earlier this year, many likely fronts for Cybercrime.

In view of the above, Information Security Education and Awareness (ISEA), Ministry of Electronics and Information Technology (MeitY), Government of India, is working to help you stay safe in the digital world throughout the COVID-19 pandemic and support internet users and employees to be aware and stay safe.

We (ISEA) reveal how to stay safe online while Working From Home (WFH) during the COVID-19 outbreak. To fight against the virus, social distancing techniques are the best solutions as per the experts. People have to opt to work remotely to self-isolate or to simply help slow the spread of the virus.

We wish all of you a very healthy and fun at home

1 Cyber Security Risk Trends reveals with respect to COVID-19

The new trend of cyber-attacks through malware and ransomware in the context of COVID-19 is 'Fearware'. The cyber attackers are exploiting the fear of coronavirus to cause the victim to fall prey to cyber-attacks.

The hackers are releasing new computing viruses and mobile applications relating to COVID-19 updates and other information. They are also designing phishing websites, emails and phishing UPI accounts in name of COVID-19, which are leading to Cyber frauds.

Organizations are responding to growing COVID-19 disruptions by allowing employees and students to work from home via the internet

The surge in inexperienced remote workers is creating a host of potential cybersecurity threats.

As organizations use VPNs [virtual private networks] for telework, more vulnerabilities are being found and targeted by malicious cyber actors.

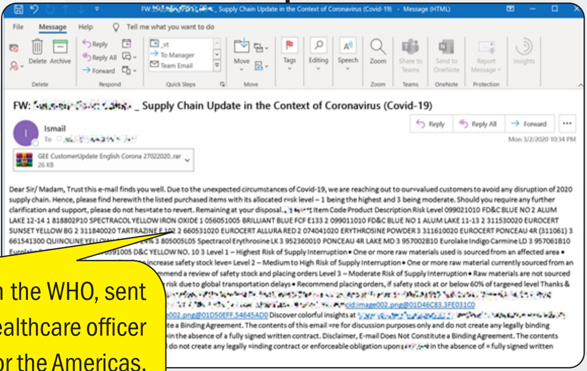
Phishing emails and messages in the name of boss are one form of cyber-attacks targeting employees working from home.

Cybercriminals are targeting the individuals in the form of the phishing attacks through emails, messages to steal sensitive & critical information and deploy additional malware through websites and mobile applications to lure internet users.

Following are some of the incidents reported in India and other countries. Some examples/ Case Studies refer about trends of Cyber Security Risks as part of COVID-19 disruption.

Example 1 :

Using World Health Organization mail in the name of COVID-19 as legit application by the fraudsters and spreading malwares to control your end devices



FW: [redacted] _ Supply Chain Update in the Context of Coronavirus (Covid-19)

Ismail

To [redacted]

Mon 3/2/2020 10:34 PM

GEE CustomerUpdate English Corona 27022020..rar
26 KB

Dear Sir/ Madam, Trust this e-mail finds you well. Due to the unexpected circumstances of Covid-19, we are reaching out to our=valued customers to avoid any disruption of 2020 supply chain. Hence, please find herewith the listed purchased items with its allocated r=sk level – 1 being the highest and 3 being moderate. Should you require any further clarification and support, please do not hes=tate to revert. Remaining at your disposal., [redacted] Item Code Product Description Risk Level 099021010 FD&C BLUE NO 2 ALUM LAKE 12-14 1 818802P10 SPECTRACOL YELLOW IRON OXIDE 1 056051005 BRILLIANT BLUE FCF E133 2 099011010 FD&C BLUE NO 1 ALUM LAKE 11-13 2 311530020 EUROCERT SUNSET YELLOW BG 2 311840020 TARTRAZINE E 102 2 660531020 EUROCERT ALLURA RED 2 074041020 ERYTHROSINE POWDER 3 311610020 EUROCERT PONCEAU 4R (311061) 3 661541300 QUINOLINE YELLOW 14% 3 805005L05 Spectracol Erythrosine LK 3 952360010 PONCEAU 4R LAKE MD 3 957002B10 Eurolake Indigo Carmine LD 3 957061B10 Eurolak 6591005 D&C YELLOW NO. 10 3 Level 1 – Highest Risk of Supply Interruption • One or more raw materials used is sourced from an affected area •

increase safety stock leve= Level 2 – Medium to High Risk of Supply Interruption • One or more raw material currently sourced from an

mmend a review of safety stock and placing orders Level 3 – Moderate Risk of Supply Interruption • Raw materials are not sourced

risk due to global transportation delays • Recommend placing orders, if safety stock at or below 60% of targe=ed level Thanks &

[redacted] cid:image002.png@01D46C83.3FE031C0

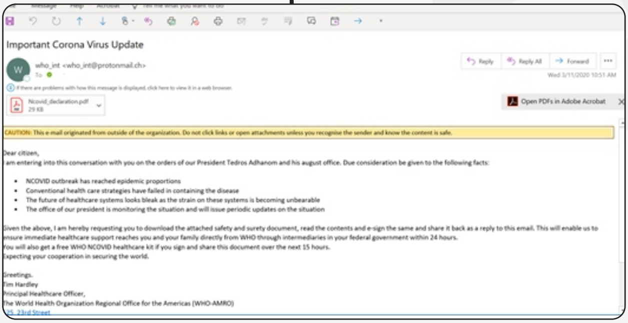
002.png@01D50EFF.54645AD0 Discover colorful insights at [redacted]

te a Binding Agreement. The contents of this email =re for discussion purposes only and do not create any legally binding

in the absence of a fully signed written contract. Disclaimer, E-mail Does Not Constitute a Binding Agreement. The contents

do not create any legally =inding contract or enforceable obligation upon [redacted] in the absence of = fully signed written

The email looks like it's from the WHO, sent by a Tim Hardley, principal healthcare officer from WHO's regional office for the Americas. A Google search throws up no results for such a WHO official.



Important Corona Virus Update

who_int <who_int@protonmail.ch>

To

Wed 3/11/2020 10:51 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

Ncovid_declaration.pdf
29 KB

CAUTION: This e-mail originated from outside of the organization. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Dear citizen,
I am entering into this conversation with you on the orders of our President Tedros Adhanom and his august office. Due consideration be given to the following facts:

- NCOVID outbreak has reached epidemic proportions
- Conventional health care strategies have failed in containing the disease
- The future of healthcare systems looks bleak as the strain on these systems is becoming unbearable
- The office of our president is monitoring the situation and will issue periodic updates on the situation

Given the above, I am hereby requesting you to download the attached safety and surety document, read the contents and e-sign the same and share it back as a reply to this email. This will enable us to ensure immediate healthcare support reaches you and your family directly from WHO through intermediaries in your federal government within 24 hours.
You will also get a free WHO NCOVID healthcare kit if you sign and share this document over the next 15 hours.
Expecting your cooperation in securing the world.

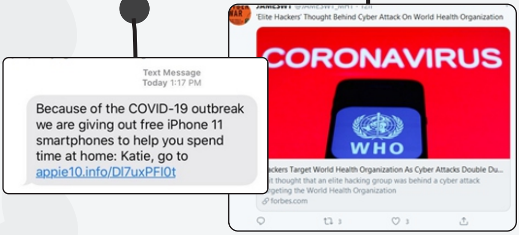
Greetings.
Tim Hardley
Principal Healthcare Officer,
The World Health Organization Regional Office for the Americas (WHO-AMRO)
25, 23rd Street

Example 2 :

Using names of trusted organizations in phishing attacks in order to attain credibility and to lure victims to further open attachment

Example 3 :

Using organization mobile applications in the name of COVID-19 as legit application by the fraudsters and spreading phishing mails/sites and fake news



Text Message
Today 1:17 PM

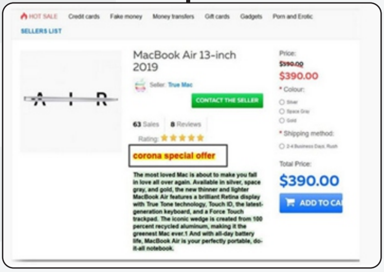
Because of the COVID-19 outbreak we are giving out free iPhone 11 smartphones to help you spend time at home: Katie, go to appie10.info/Dl7uxPFI0t

JAMESWT @JAMESWT_MHT · 12h
'Elite Hackers' Thought Behind Cyber Attack On World Health Organization

ackers Target World Health Organization As Cyber Attacks Double Du...
it thought that an elite hacking group was behind a cyber attack
rgeting the World Health Organization
forbes.com

Example 4 :

- Offering discount by sending promotional codes & also sending legitimate information on Coronavirus Maps may attract viruses and financial frauds.
- Coupons or promotional codes such as "Coronavirus" codes or "CoronaVirus Discount! 10% off ALL products"
- A hacking group named "SSHacker" is offering Facebook account hacking services with a 15% discount with promotional code "COVID-19" on DeepDotMarket.



MacBook Air 13-inch 2019

Seller: True Mac

63 Sales 8 Reviews
Rating: ★★★★★

corona special offer

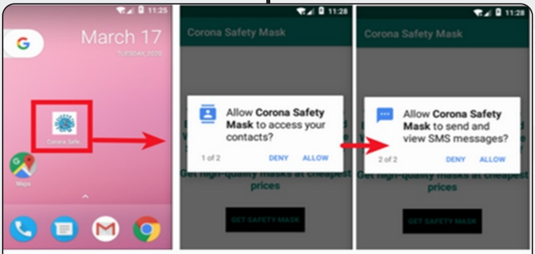
The most loved Mac is about to make you fall in love all over again. Available in silver, space gray, and gold, the new thinner and lighter MacBook Air features a brilliant Retina display with True Tone technology, Touch ID, the latest-generation keyboard, and a Force Touch trackpad. The iconic wedge is created from 100 percent recycled aluminum, making it the greenest Mac ever.1 And with all-day battery life, MacBook Air is your perfectly portable, do-it-all notebook.

Price:
~~$390.00~~
$390.00

- Colour:
○ Silver
○ Space Gray
○ Gold

- Shipping method:
○ 2-4 Business Days, Rush

Total Price:
$390.00



Allow **Corona Safety Mask** to access your contacts?
1 of 2 DENY ALLOW

Allow **Corona Safety Mask** to send and view SMS messages?
2 of 2 DENY ALLOW

ndroid app called Corona Safe steals your contacts and spams your riends, warns Zscaler. ZSCALER

Example 5 :

Malware being delivered via Android apps that steal victims ? offering Coronavirus safety mask upon installation

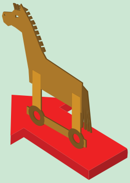
Criminals are misusing the search data and curiosity related to Coronavirus. Be vigilant on messages, emails and websites. Cyber Criminals can remotely access people's sensitive information and bank transactions

2 Malware and Ransomware families related to COVID -19

The following are few of the malware and ransomware families in the context of COVID-19.

Emotet Trojan

Emotet is a Trojan that is primarily spread through spam emails (malspam). The infection may arrive either via malicious script, macro-enabled document files, or malicious link. Emotet emails may contain familiar branding designed to look like a legitimate email. Though its old Trojan these trojans visible during this COVID-19 crisis



Maze ransomware attackers extort vaccine testing facility

The cybercriminal gang behind Maze ransomware has been extorting a UK-based clinical research organization that has been preparing to play a potential role in testing vaccine candidates for the novel Coronavirus despite assurances that they would not harm any healthcare organizations during the COVID-19 crisis

Agent Telsa

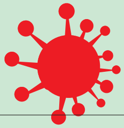
Agent Tesla collects account information from the victim's machine. It can steal data from the victim's clipboard and encrypts the data with 3DES before sending it over the C2 server. As the employees' working from home use Internet for various official activities this AgentTesla keyloggers are used by cyber attackers to steal sensitive information

Ransomware 'Locky'

The variant of Locky ransomware was found in most of the fake emails connected with the outbreak

Covidlock

A new type of ransomware known as CovidLock encrypts key data on an Android device and denies access to the victims unless they pay up



AZORult

Adversaries have created a weaponized coronavirus map app that infects victims with a variant of the information-stealing AZORult malware

TrickBot

The TrickBot banking malware have developed an Android app that can bypass some of the two-factor authentication (2FA) solutions employed by banks. This Android app, named TrickMo, works by intercepting one-time password (OTP) codes banks send to users via SMS or push notifications. TrickMo collects and then sends the codes to the internet crooks to bypass logins or authorize fraudulent transactions.

Lokibot

LokiBot is trojan-type malware designed to infiltrate systems and collect a wide range of information. ... LokiBot typically infiltrates systems without users' consent - it is distributed via spam emails (Windows OS), various private messages (SMS, Skype, etc.), and malicious websites

Nanocore RAT

Nanocore is a remote access Trojan virus otherwise known as RAT Malware which is used in both targeted and non-targeted attacks. A RAT or Remote Administration Tool, is a software that gives a person full control over a tech device, remotely. The RAT gives the user access to your system, just as if they had physical access to your the device and found campaigns using COVID-19 fears to distribute the Nanocore RAT

3 Online threats that people may encounter working remotely

The online threats that people working remotely should be aware of during the pandemic COVID- 19, which have been observed during this outbreak are:

Unsecured Wi-Fi networks:

Personal Wi-Fi networks installed at home can be controlled to make it secure. However, if it is chosen to use public Wi-Fi networks it may lead to sniffing/monitoring your internet activities by unintended users as public Wi-Fi networks are primary spots for malicious users to spy on Internet traffic and collect confidential information.

Remember Most of the Wi-Fi networks normally use the 'WEP' open authentication that is unsecure. This type of encryption has many security flaws that can cause your personal information, through your network traffic, to be seen. Your home network can also be flagged as unsecured if the encryption type is set to 'WEP’

For more details, please visit: https://www.infosecawareness.in/concept/wifi-security?lang=en

Here are few simple things that you should do to secure your wireless network:

- Open your router settings page
- Create a unique and strong password for your router administration interface and for your SSID
- Change your Network's SSID name
- Enable Highest Network Encryption which your router supports
- Filter MAC addresses
- Reduce the Range of the Wireless Signal
- Upgrade your Router's firmware regularly.

For more information, please visit: www.infosecawareness.in/wifi-security

Using personal devices and networks:

Many employees may be using the personal devices as hotspots for complete work schedules in case of non-availability of Wi-Fi. Users may not hesitate to connect to a mobile hotspot, but that doesn't mean it should always allow it. Learn what threats these hotspots pose and how to handle them.

Whenever you connect to the Internet through mobile hotspot—no matter whether you're using a laptop, phone, or tablet- you may encounter unknown members in your network or hackers who access your mobile internet without your permission. If you and everyone who shares access to the internet using your mobile hotspot (including strangers) exceed the data limit in your plan, you're the one who gets the bill for the excess data usage. Avoid this scenario by bolstering the security of your mobile hotspot. All possible threats for a regular Wi-Fi network are also applicable to the mobile hotspot.

The personal devices lack the tools built in to business networks such as strong antivirus software, customized firewalls and automatic online backup tools. This increases the risk of malware finding its way onto devices and thus both personal and work-related information can be compromised.

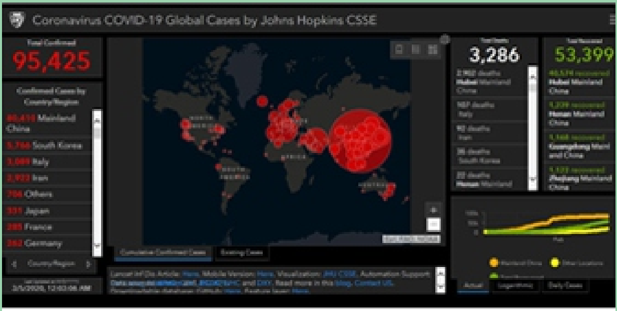
Here are few simple things that you should do to secure your personal hotspot

- Enable Strong Encryption on Your Hotspot
- Change Your Hotspot's SSID
- Create a Strong Wireless Network Password (Pre-shared Key)
- Enable Your Hotspot's Port-Filtering and Blocking Features
- Don't Give Out Your Network Password and Change It Often
- Restrict number of devices connected to the hotspot
- Refresh your hotspot and check for other devices if connected
- Disconnect the internet service if not in use

Thankfully, armed with the right knowledge and tools, you can avoid many of these threats and continue getting the work done.

Some more examples and indications of attacks by fraudsters during COVID -19

Example 1 :

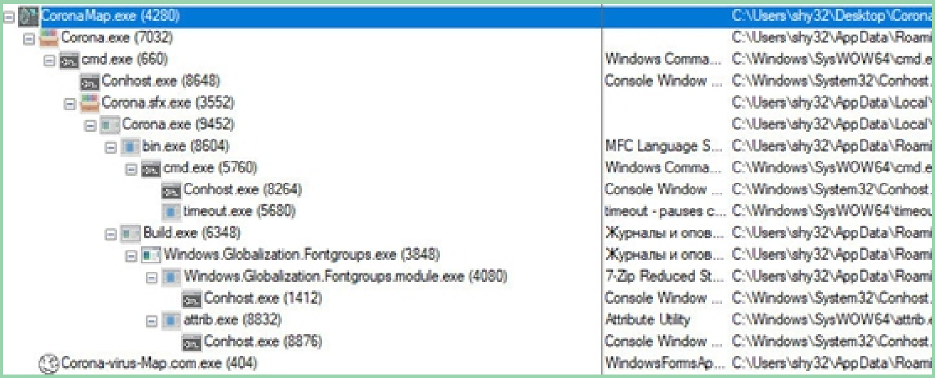


Beware of 'Coronavirus Maps' – It's a malware infecting PCs to steal passwords

- Cybercriminals will stop at nothing to exploit every chance to prey on internet users.
- Even the disastrous spread of COVID-19 (the disease), is becoming has become an opportunity for them to likewise spread malware or launch cyber-attacks.
- The malware attack specifically aims to target those who are looking for cartographic presentations of the spread of COVID-19 on the Internet, and tricks them to download and run a malicious application that, on its front-end, shows a map loaded from a legit online source but in the background compromises the computer.

Signs of Infection :

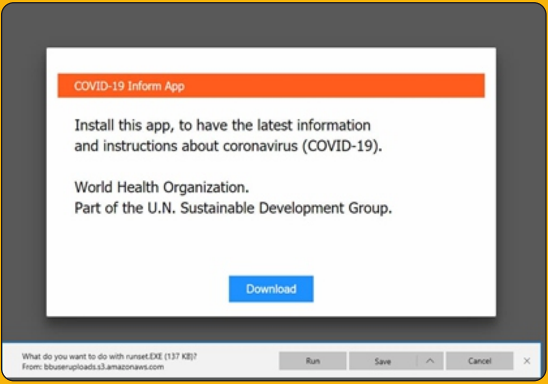
Executing the Corona-virus-Map.com.exe results in the creation of duplicates of the Corona-virus-Map.com.exe file and multiple Corona.exe, Bin.exe, Build.exe, and indows.Globalization. Fontgroups.exe files.



```
⊟ CoronaMap.exe (4280)                                                            C:\Users\shy32\Desktop\Corona
  ⊟ Corona.exe (7032)                                                             C:\Users\shy32\AppData\Roami
    ⊟ cmd.exe (660)                                           Windows Comma...   C:\Windows\SysWOW64\cmd.e
        Conhost.exe (8648)                                    Console Window ...  C:\Windows\System32\Conhost.
      ⊟ Corona.sfx.exe (3552)                                                     C:\Users\shy32\AppData\Local\
        ⊟ Corona.exe (9452)                                                       C:\Users\shy32\AppData\Local\
          ⊟ bin.exe (8604)                                    MFC Language S...   C:\Users\shy32\AppData\Roami
            ⊟ cmd.exe (5760)                                  Windows Comma...    C:\Windows\SysWOW64\cmd.e
                Conhost.exe (8264)                            Console Window ...  C:\Windows\System32\Conhost.
                timeout.exe (5680)                            timeout - pauses c... C:\Windows\SysWOW64\timeou
          ⊟ Build.exe (6348)                                  Журналы и опов...   C:\Users\shy32\AppData\Roami
            ⊟ Windows.Globalization.Fontgroups.exe (3848)     Журналы и опов...   C:\Users\shy32\AppData\Roami
              ⊟ Windows.Globalization.Fontgroups.module.exe (4080) 7-Zip Reduced St... C:\Users\shy32\AppData\Roami
                  Conhost.exe (1412)                          Console Window ...  C:\Windows\System32\Conhost.
              ⊟ attrib.exe (8832)                             Attribute Utility   C:\Windows\SysWOW64\attrib.
                  Conhost.exe (8876)                          Console Window ...  C:\Windows\System32\Conhost.
    Corona-virus-Map.com.exe (404)                            WindowsFormsAp...   C:\Users\shy32\AppData\Roami
```

Example 2 :

Hackers Hijack Routers' DNS to Spread Malicious COVID-19 Apps



COVID-19 Inform App

Install this app, to have the latest information and instructions about coronavirus (COVID-19).

World Health Organization.
Part of the U.N. Sustainable Development Group.

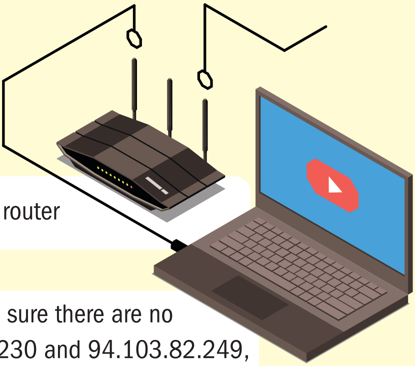
What do you want to do with runset.EXE (137 KB)?
From: bbuseruploads.s3.amazonaws.com

- A new cyber-attack is hijacking router's DNS settings so that web browsers display alerts for a fake COVID-19 information app from the World Health Organization that is the Oski information-stealing malware.
- The malware opens the web browser on its own (while installing the mobile application) and displays a message prompting them to download a 'COVID-19 Inform App' that was allegedly from the World Health Organization (WHO).
- These alerts were being caused by an attack that changed the DNS servers configured on their home D-Link or Linksys routers to use DNS servers operated by the attackers.
- If a user downloads and installs the application, instead of receiving a COVID-19 information application they will have the Oski information-stealing Trojan installed on their computer.
- When launched, this malware will attempt to steal the following information from the victim's computer:
  - browser cookies
  - browser history
  - browser payment information
  - saved login credentials
  - cryptocurrency wallets
  - text files
  - browser form autofill information
  - Authy 2FA authenticator databases
  - a screenshot of your desktop at the time of infection, and more.

What you should do if affected by this attack ?

If your browser is randomly opening to a page promoting a COVID-19 information app, then you need to login to your router and make sure you configure it to automatically receive its DNS servers from your ISP.

As every router has a different way of configuring DNS servers, it is not possible to give a specific method on how to do this.



In general, you will want to follow these steps:

Login to your router

Find the DNS settings and make sure there are no servers, especially 109.234.35.230 and 94.103.82.249, manually configured. If they are, set the DNS servers setting to 'Automatic' or ISP assigned.

Then save your configuration

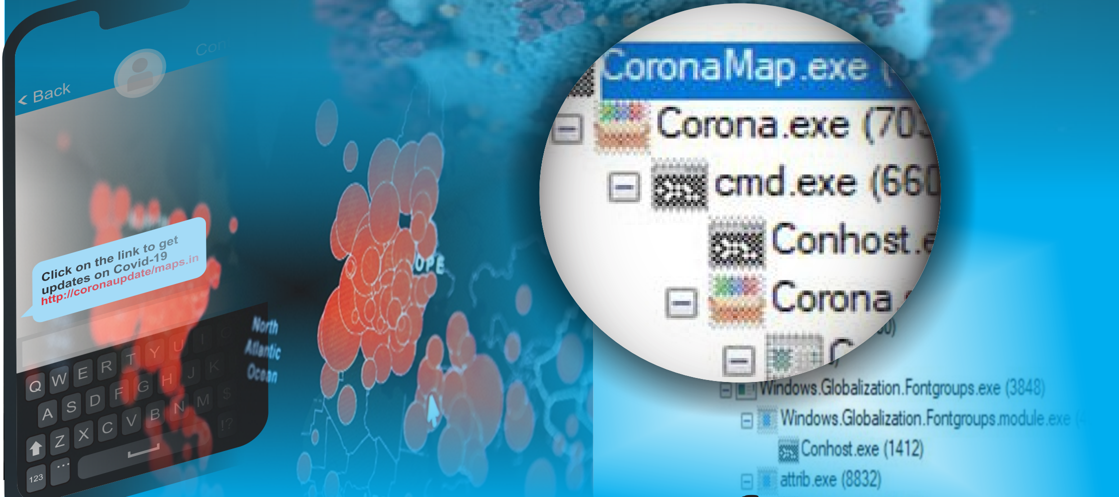
- Reboot mobile devices, game consoles, and computers so that they use the correct DNS settings from ISP.
- As people are reporting that they think their settings were changed because of a weak password and that remote administration was enabled, it is important to change your password to something stronger and to disable remote administration on the router.
- Finally, if you downloaded and installed the COVID-19 app, you should immediately perform a scan on your computer for malware.
- Once clean, change all of the passwords for sites whose credentials are saved in your browser and you should change the passwords for any site that you visited since being infected.
- When resetting your passwords, be sure to use a unique password at every site.

Information Security
Education & Awareness
www.isea.gov.in

For more details visit :
www.InfoSecawareness.in

Malware Attacks

in light of COVID-19 pandemic



< Back
Click on the link to get updates on Covid-19 http://coronaupdate/maps.in
North Atlantic Ocean
CoronaMap.exe
Corona.exe (70
cmd.exe (66
Conhost.e
Corona
Windows.Globalization.Fontgroups.exe (3848)
Windows.Globalization.Fontgroups.module.exe
Conhost.exe (1412)
attrib.exe (8832)
Conhost.exe (8876)

Beware of

Coronavirus Virus Spread Maps

It's a malware infecting PCs to steal passwords

The disastrous spread of COVID-19 is becoming an opportunity for the cybercriminals to spread malware or launch cyber attacks

Avoid clicking on any unknown messages with
links/ install application from unknown sources
Keep your personal information safe
Don't use open Wi-Fi
Use strong and different passwords for different accounts
Install updated Anti-Virus/Malware Software

For more information, please visit: www.infosecawarenees.in

Programme by : Ministry of Electronics & Information Technology(MeitY), Govt. of India

Supported by : Ministry of Home Affairs (MHA), Govt. of India

For Virus Alerts,Incident & Vulnerability Reporting
cert-in
Handling Computer Security Incidents
http://cert-in.org.in/

www.
cyberswachhtakendra.
gov.in

CYBER DOST

Cyber Safe GIRL
Beti Bachao, Cyber Crime Se...

END NOW FOUNDATION
ADVOCACY ON CYBER SAFETY

For more details / queries on
Cyber Security
Call us on our Toll free No.
1800 425 6235

Implemented by
सी डैक
CDAC

4 Recommendation of Best Practices to be followed by users to stay safe online:

While working from home in this situation (COVID-19 lock down period), ensure that you abide by the security measures taken by organization. Also, follow the directions given by your organisation on how to handle certain cybersecurity aspects; they may also provide you access to some security tools needed to protect yourself while working from home.

The following safety guidelines may help you to secure yourself while working from home.

Password Security:

First and foremost, ensure use of strong passwords for your Wi-Fi network, system, email accounts, remote desktop systems, VPN connection etc.

To ensure strong passwords: Use at least eight characters for strong password, avoid Dictionary Words and the once ones which bad guys can guess; use characters from at least three of the following four classes: English upper case letters, English lower case letters, Westernized Arabic numerals (0,1,2,...) Non-alphanumeric (special) characters such as punctuation symbols.

Enable two factor authentication to ensure security

Two-factor authentication methods rely on a user providing a password, as well as a second factor, usually either a security token or a biometric factor, such as a fingerprint or facial scan.

Where you can use 2FA

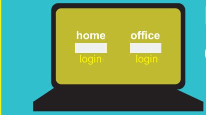
You can enable 2FA on most of your online accounts, like your:

- email accounts
- social media networks
- internet banking
- online shopping sites.
- You can also set 2FA up on your devices — on laptops, tablets, smartphones, and even some game consoles

Do not share the passwords/ systems allocated with the family members.

For more details, please visit: [https://www.infosecawareness.in/concept/good-and-strong-password?lang=en]

Use separate login users for your system if you are using personal computer for work from home



If personal computer is used at home for carrying out official work, then it is certain you maintain official files on your personal computer. To avoid loss of data or revealing official information to family members, it is preferred to use separate login users for your home systems

Network Security:

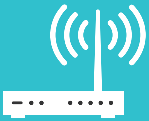
Use VPN (Virtual Private Network) through organization provided hardware only.

- Use Virtual Private Network (VPN) only on company-provided hardware with up-to-date security features, else infected data may transmit over VPN to subsequent networks of your organization if the your system is infected/compromised.

Set up firewalls

- Enable firewalls which act as a line of defence to prevent threats entering the system. They create a barrier between the device and the internet by closing ports to communication. This can help prevent malicious programs entering and can stop data leakage
  from the device.

Secure your home router



It is important to take simple steps to protect your home network to prevent malicious parties having access to connected devices. Changing your router password is a good first step, but there are other actions you can take. For example, you should make sure firmware updates are installed so that security vulnerabilities can be patched. The encryption should be set to WPA2 or WPA3. Restrict inbound and outbound traffic, use the highest level of encryption available

Wi-Fi Connectivity

Ensure you use a secure Wi-Fi network to connect to your organisation network. Avoid Public Hotspots or open Wi-Fi.

Closure of Unwanted Ports

It is highly recommended to close unnecessary network ports with the help of your IT/Security teams. Also, turn off networking capabilities (such as Bluetooth and Wi-Fi) for mobile and laptop when not necessary for work

For more details, please visit https://www.infosecawareness.in/concept/wifi-security

Data Security

- Continuously back up your data into separate devices as you may be safe with this data in case of any ransomware attacks. Better to back-up your official data on daily basis.
- Use encrypted communications
- Disable use of Macros in Microsoft office, as COVID-19 malwares are mostly using VBA Macros as an initial step for targeting victims.
- Non-technical staff, while working from home, should take care of the confidentiality of valuable transactions and sensitive financial documents.
- Securing the data while transmitting it includes encryption and authentication and also the end-to-end users are authorized. Encryption plays an important role in securing many different types of information technology (IT) assets. It provides the Confidentiality which encodes the message's content, Authentication verifies the origin of a message and Integrity proves the contents of a message have not been changed since it was sent.

For more details, please visit: https://www.infosecawareness.in/concept/family/data-security

Remote Access Security

Remote desktop: is a program or an Operating System feature that allows a user to connect to a computer in another location, computer's desktop and interact with it as if it were local.

It is noteworthy to document remote access requirements:

- Authorize remote access before allowing connections, monitor and control remote access.
- Encrypt remote access connections from the organization's firewall and threat detection.
- Ensure employee' systems/desktops are fully protected and has the same protection as office workstations.

Virtual Desktop: The work from home employees need to access project / company data and applications through a browser-based webpage or virtual desktop.

- Ensure that all applications and data are stored on the portal's server and cannot be downloaded or saved on an employee's device without permission. This is a good way to keep control over accessing your data and how it is used.
- Make it mandatory to restrict employee's access to other programs while the portal is in use else there may be a high risk of over exposure.

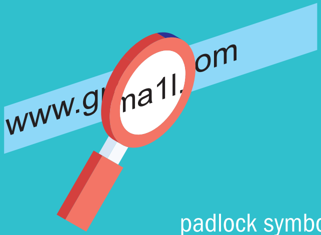
Risk Assessment:

- Risk assessment should be performed as part of selecting a remote access method (application portals, remote desktop access, direct application access).

Look out for phishing emails and sites

With the rise in the number of people working from home due to the Coronavirus outbreak, no doubt there will be plenty of Cybercriminals looking to cash in on the trend. It's highly likely that phishing emails will target remote workers in a bid to steal their personal information or gain access to company accounts.

- Avoid clicking on links in unsolicited emails and email attachments: To spot a phishing email, cross check the sender's email address for spelling errors and look for poor grammar in the subject line and email body. Hover over links to see the URL and don't click links or attachments.



- Even if a link is clicked and end up on a legitimate-looking site, be sure to check its credibility before entering any information.
- Common signs of a phishing site include lack of an HTTPS padlock symbol (although phishing sites increasingly have SSL certificates), misspelled domain names, poor spelling and grammar, lack of an "about" page, and missing contact information.

Tips to Remember :

- Review emails carefully for grammar and spelling mistakes or any other suspicious signs.
- Do not open links or attachments from unknown parties.
- Never Go to Your Bank's Website by Clicking on Links Included in Emails
- Enter your username and password only over a secure connection. Look for the "https" prefix before the site URL, indicating the connection to the site is secure.
- Be cautious about opening any attachments or downloading files you receive regardless of who sent them.
- Look for the sender email ID before you enter/give away any personal information.
- Use antivirus, antispyware and firewall software (update them regularly too).
- Always update your web browser and enable phishing filter.

For Virus Alerts,Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents
http://cert-in.org.in/

Device Security

Lock device when not in use: Password-locking the device while leaving your system so that unauthorized access to your data can be avoided

Tips to Remember :

- Install updates regularly
- Use an updated antivirus software for filtering malwares :
- A good & up to date antivirus software can act as the next line of defence by detecting and blocking known malware
- with remote access policy configuration for auto-update of virus definition, your machine should be properly patched before connecting to your organisation network.
- If you’re looking for more protection, use an additional full disk encryption tools (Ex: VeraCrypt or BitLocker etc)

For more details, please visit: https://www.infosecawareness.in/topic/desktop-security

Staying safe and Secure in the Time of COVID-19

It's amply clear that these attacks exploit Coronavirus fears and people's hunger for information about the outbreak. Given the impact on the security of businesses and individuals alike, it' is essential to avoid falling victim to online scams and practice good digital hygiene:

Businesses should ensure that secure remote access technologies are in place and configured correctly, including the use of multi-factor authentication, so that employees can conduct business just as securely from home.

- Individuals should keep away from using unauthorized personal devices for work, and ensure personal devices have the same level of security as a company-owned device, and also consider the privacy implications of employee-owned devices connecting to a business network."
- Watch out for emails and files received from unknown senders. Most importantly, check a sender's email address for authenticity, don't open unknown attachments or click on suspicious links, and avoid emails that ask them to share sensitive data such as account passwords or bank information.
- Use trusted sources, such as legitimate government websites — for up-to-date, fact-based information about COVID-19.

Authorised Websites for info on COVID-19 related :
https://www.mohfw.gov.in/
https://www.who.int/india/emergencies/novel-coronavirus-2019

Subscribe us at
/c/InformationSecurityEducationandAwareness

Follow us at
/InfoSecAwa

Connect us with
/infosecawareness

Follow us at
/infosec_awareness

About ISEA

Looking at the growing importance for the Information Security, Ministry of Electronics & Information Technology has identified this as a critical area. Information Security Education and Awareness (ISEA) Project was formulated and launched by the Govt. of India. One of the activities under this programme is to spread Information Security Awareness among children, teachers, home users, IT and non-IT professionals throughout the country. C-DAC Hyderabad has been assigned the responsibility of executing this project by Ministry of Electronics & Information Technology, Government of India. As part of this activity C-DAC, Hyderabad has been preparing Information Security Awareness material, coordinating with Participating Institutes (PI's) in organizing the various Information Security Awareness events all over India.

To Share Tips / Latest News, mail us to

isea@cdac.in

ISEA Whatsapp Number for Incident Reporting

+91 9490771800

between 9.00 AM to 5.30 PM

For queries on Information security

Call us on Toll Free No.

1800 425 6235

सत्यमेव जयते

Ministry of Electronics &
Information Technology,
Government of India

सी डैक
CDAC

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India

Plot No: 6&7, Hardware Park Sy. No.1/1, Srisailam Highway Raviryal (V & GP), Via Ragaanna guda,
Maheshwaram (M), Ranga Reddy District, Hyderabad – 501510. Tel: 9248920201.