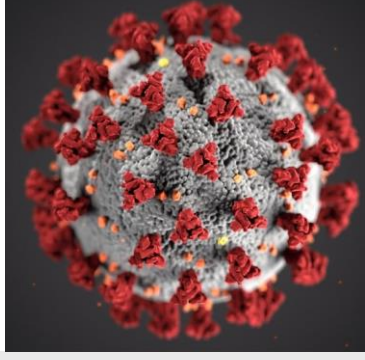
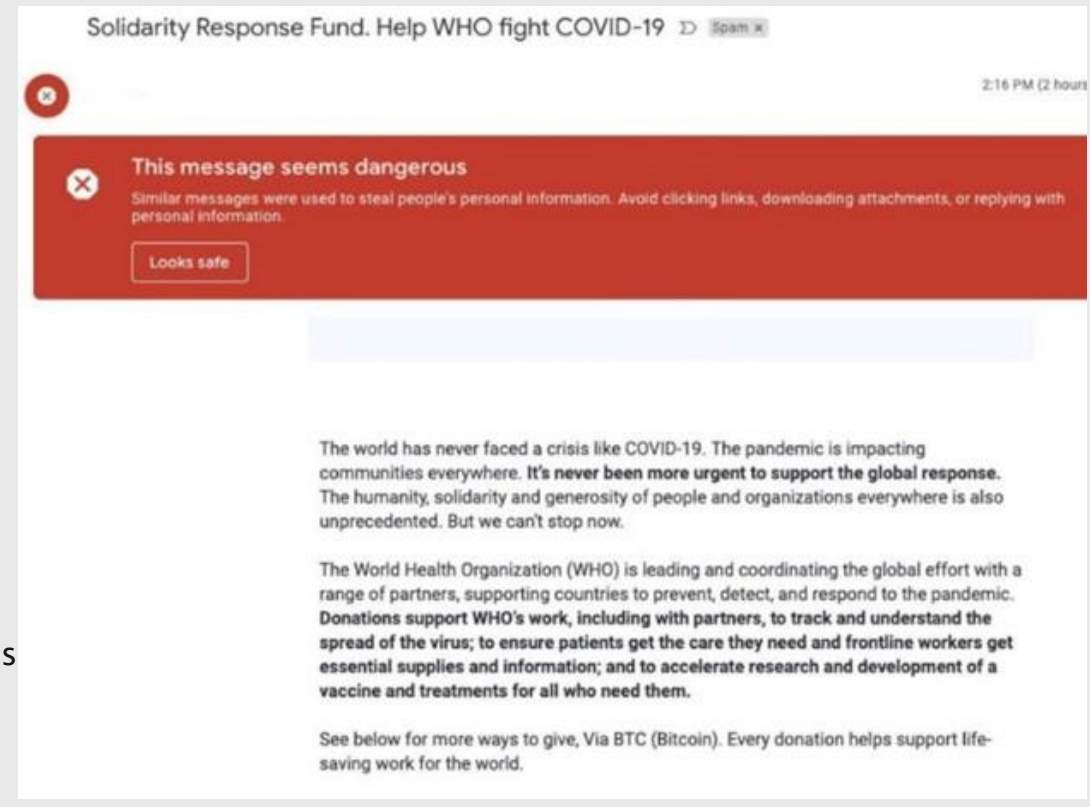
CYBER ATTACKS DURING COVID19 AND PRECAUTIONS TO BE TAKEN



PHISHING ATTACKS



Emails are sent to very large numbers of recipients and groups, and typically is random , luring the receiver into revealing sensitive information through mails

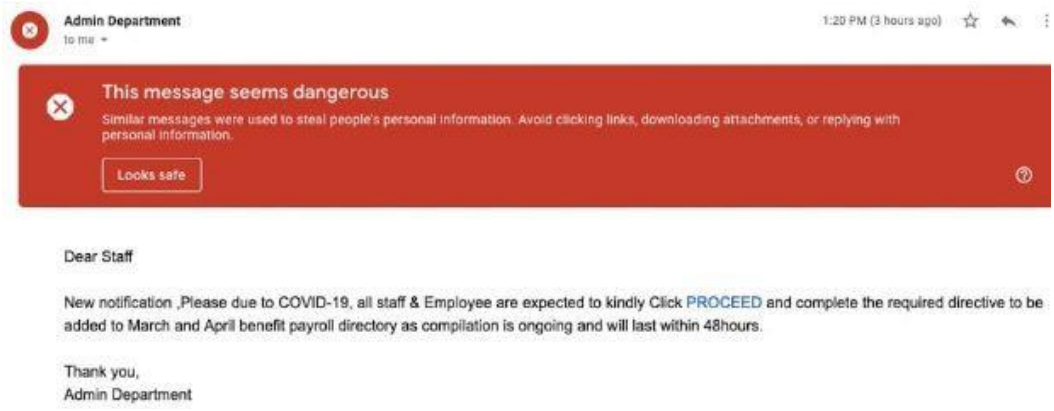
EXAMPLE:

Mail Stating; “The world has never faced a pandemic like COVID19.Click here to support Migrant workers, Sanitary Workers in BTC. Let’s stand together”.

PRECAUTIONS

1. Examine the sender's email address to **ensure if it is from a true account**. Hover over the link to expose the associated web addresses in the “to” and “from” fields;
2. **Note grammatical errors** in the text of the email; they are usually a sure sign of fraud.

SPEAR- PHISHING ATTACKS



Carefully crafted fake email targeted to an individual mails in an attempt to obtain sensitive information like passwords, account details or expecting monetary favoursand are very common in enterprise scenarios.

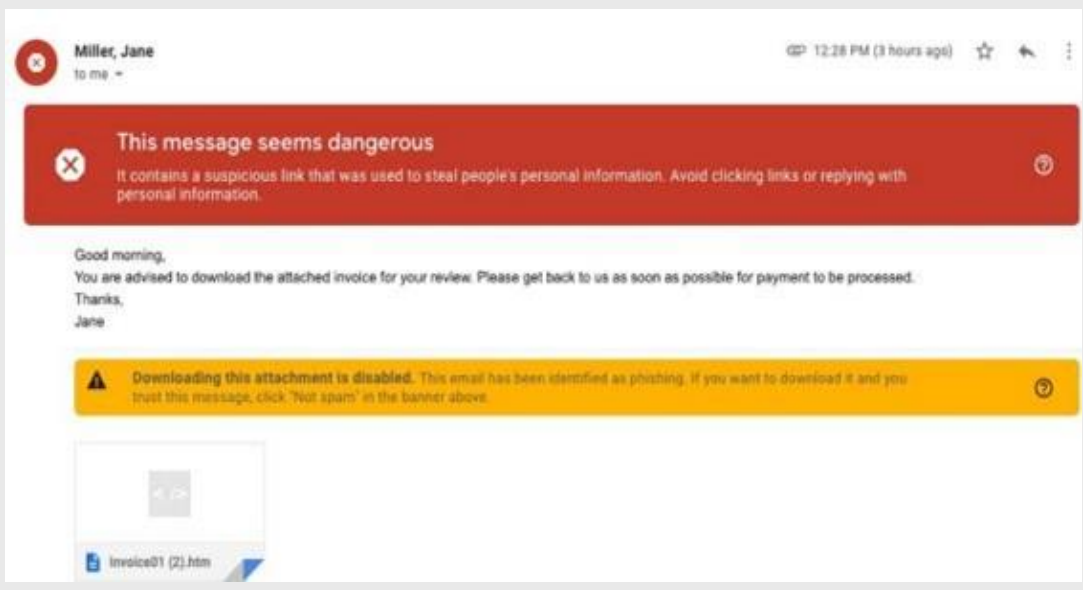
EXAMPLE

Mails stating,
“Dear Staff,
The employees are requested to click the link to complete the directive within 36 hours for adding into March-April payroll directory".

PRECAUTIONS

1. Examine the sender’s email.
2. **Report suspicious emails** to the IT / Security department of the Organization.
3. **Don't forward** suspicious emails to co-workers

MALWARE ATTACKS



Asks the user to download attachments claiming to be official notifications released by WHO and other known Organization.

EXAMPLE

- Email impersonating WHO that claims to have documents attached that includes latest news on COVID19 vaccine release. The attachment may be a rar archive, doc, pdf that includes .exe file which is a Nanocore RAT malware.

PRECAUTIONS

1. **Be skeptical** of pop-ups, emails from unknown senders.
2. **Don't click** on links or open attachments from those senders.
3. **Use updated version** of Antivirus

RANSOMWARE ATTACKS

Asks the users to enable macros to view the downloaded attachments. Once enabled, encrypts the entire file system and demands the user to pay in BTC to decrypt the files.

EXAMPLE

- Zeus Sphinx that surfaced three years ago is attempting again through mails claiming to offer financial relief.

PRECAUTIONS

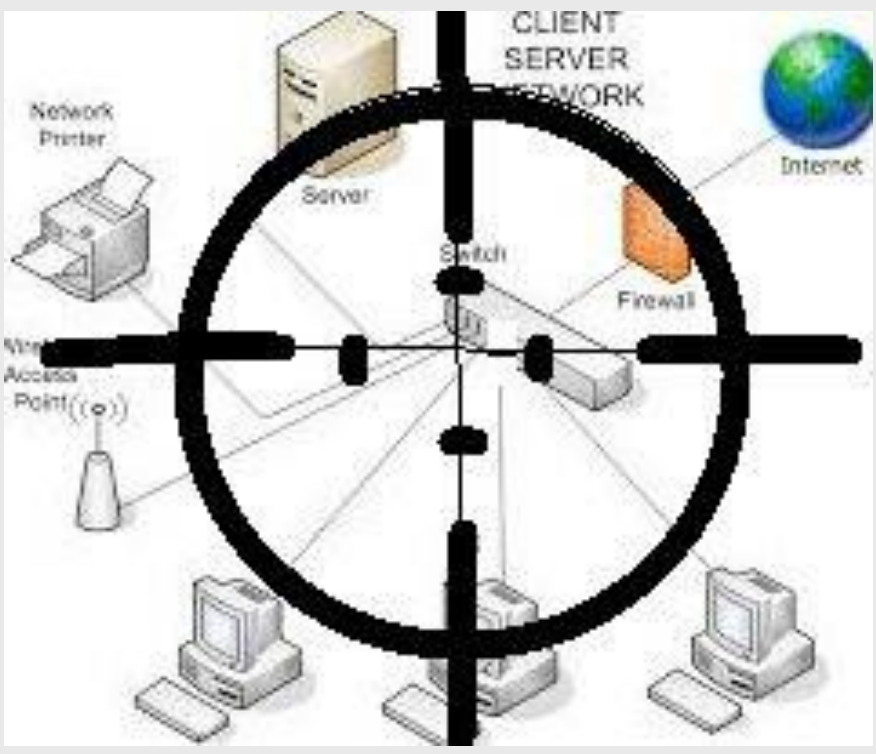
1. **Disable Macros** while using Microsoft Office.
2. Maintain **Periodic Back-ups.**

TARGETED ATTACKS

Threat actors focus only on compromising a specific entity over a period of time.

EXAMPLE

- Hackers have forced the Italian social security website to shut down for a period.



PRECAUTIONS

1. **Secure your Wi-Fi access point**. Change default settings and default passwords in order to secure your home network.
2. **Avoid accessing social networks** like Facebook, Twitter etc., from the system that you access the office network.
3. **Do not connect to public/open Wi-Fi networks**. Use a separate home internet network for work to isolate personal devices.
4. **'Remember password' function should always be turned off** when you are logging intoyour organization'ssystems from your personal devices.
5. **Strengthen your remote access management policy and procedures**. Implement multifactor authentication for VPN access, IP address white listing, limits on remotedesktop protocol (RDP) access.

FAKE NEWS

Fake news, video clips, GIFs, authentic-looking federal government alerts connected to coronavirus (COVID-19) has been making rounds in the internet.

EXAMPLE

Messages stating,

- "Vaccine for COVID19 found and can be made at home".

- Fake Messages making rounds on the internet stating,
  "Rs.5000 will be credited as part of COVID Relief Measures"

PRECAUTIONS

1. **Do not forward messages without verifying** the credibility and authenticity of the message

VIDEO-BOMBING

People unrelated to the user groups are found to be appearing/joining the calls made via video conferencing app

EXAMPLE

- Zoom-bombing conferencecalls has become more common.

PRECAUTIONS

1. Using alternative audio and video conferencing environments like **Microsoft Teams,Google Meet and Rocketchat** and open source alternatives include **Jitsi** for communication with colleagues.

DENIAL-OF-SERVICE AND DISTRIBUTED DENIAL-OF-SERVICE ATTACKS

Attackers/Group of attackers make subsequent request to servers preventing the legitimate users from availingthe service

EXAMPLE

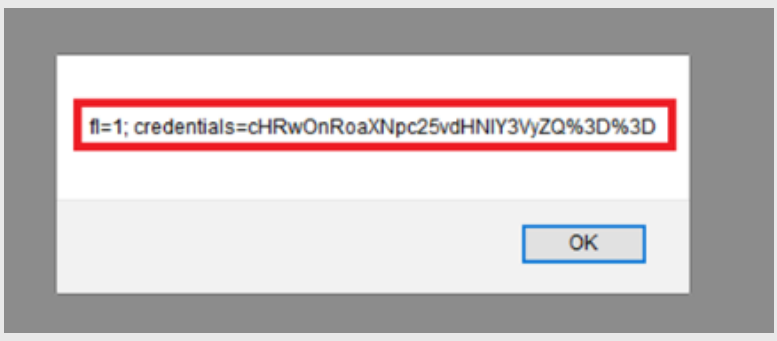
- Video-Conferencing apps have been targeted in the recent times.

PRECAUTIONS

1. **Monitoring the traffic** that ingress the server and employing end-point security devices.

CROSS-SITE SCRIPTING ATTACKS

The attacker could send the victim a misleading email with a link containing malicious JavaScript. If the victim clicks on the link, the HTTP request is initiated from the victim's browser and sent to the vulnerable web application. The malicious JavaScript is then reflected back to the victim's browser, where it is executed in the context of the victim user's session.



EXAMPLE

Mail Stating;

"Pay just Re.1 to contribute to COVID Relief fund by clicking on the link".Clicking the link takes the user to the user's net banking site asking the user to input passwords.The attacker could steal the passwords of the victim when the victim click on link.

PRECAUTIONS

1. **Ensure the authenticity** of the links and do not pay to charity from unknown charity fund collectors.

DRIVE-BY ATTACKS

When a visitor navigates to a site that injects malware onto the victim's PC, runs in the background invisible to the user without the user taking any conscious action steps to initiate the attack.

EXAMPLE

- Domain names of sites crafted to appear like the authentic websites might contain drive by downloads
- http://covidmedicine.amazon.in

PRECAUTIONS

1. Do not visit HTTP sites .
2. **Update systems and software**. Install updates and patches in a timely manner, on mobile devicesand other non-corporate devices you might use for work.
3. **Do not leave your systems unattended** at home. Creating a separate user for your system might be helpful if your laptop is going to be used by other members of the family.
4. **Install Organization-approved Anti-phishing filters** on browsers, USB media devices and to scan attachments. Indigenous tools like USB-Pratirodh, AppSamvid, JS Guard by C-DAC come in handy

References:

1. https://infosecawareness.in/article/covid19-cyber-attacks
2. https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond
3. https://www.securitymagazine.com/articles/92157-coronavirus-related-spear-phishing-attacks-see-667-increase-in-march-2020
4. https://www.forbes.com/sites/leemathews/2020/03/31/criminals-resurrect-a-banking-trojan-to-push-covid-19-relief-payment-scam/
5. https://twitter.com/MBThreatIntel/status/1247669823405830144