COVID-19 has provided many new opportunities for cyber threat.

As staff are working from home, there has been a measurable increases in spam and impersonation attack campaigns.

### Threat categories

- **Spam/ opportunistic detections**
  - Increased by 26.3%

- **Impersonation detections**
  - Increased by 30.3%

- **Malware detections**
  - Increased by 35.16%

- **Blocking of URL clicks**
  - Increased by 55.8%

*Source: [www.mimecast.com](http://www.mimecast.com)*
How the Scam Works:
1. You receive an email claiming that your device/account has been compromised.
2. Scammer claims to have your 'private and confidential' information.
3. A ransom is demanded to keep the information private.
4. Scammer may use your email and password from past data breaches as 'proof' that the email is legitimate.

What Should You Do?
- Do not make payment. Delete the email immediately.
- To prevent unauthorised access, you should:
  - Use the Latest Zoom Application
  - Secure Your Meeting
  - Manage Meeting Access
  - Update Your Devices

Use the Latest Zoom Application
Download the app from the official website and install updates immediately when available.

Secure Your Meeting
Require registration, password access and generate a unique ID for meetings. Do share ID and password with intended participants only. Use a strong password.

Manage Meeting Access
Enable the waiting room feature, disable 'join before host' option and remove any unknown participants. Lock the meeting once everyone has joined.

Update Your Devices
Ensure that the OS and anti-virus software of the device(s) installed with Zoom are updated.

Want to learn more?
Visit www.csa.gov.sg

Implementing a Remote Work Policy?
Stay cyber-safe with these tips

1. Stay Updated
   - Update all VPN, network infrastructure and endpoint devices to the latest patches

2. Set Authentication
   - Enable Multi-factor Authentication for all VPN connections

3. Secure Your Systems
   - Follow good practices guidelines recommended by solution providers

4. Audit Regularly
   - Check privileged domain and local system accounts routinely to detect unknown accounts

5. Spread Awareness
   - Provide regular reminders to employees about cyber threats and preventive measures

6. Enforce Policies
   - Impose strict security policies such as the frequency of changing and strength of passwords

7. Respond and Recover
   - Ensure cyber incident response and recovery plans are ready and can be effectively implemented

Source: www.csa.gov.sg
What you can do to protect yourself

- Employ proper cyber hygiene
- Update home WiFi with a strong password
- Never click on COVID-19 related attachments
- Right click emails to ensure the links are the correct domain
- Use 2 FA to access personal emails, etc
WANNACRY – THE RANSOMWARE EVENT OF 2017 SO FAR

- The sweeping WannaCry ransomware event that commenced on 12 May 2017 has been revealed to use two separate previously leaked Equation Group tools, and the current strain—but by no means the final strain—has been effectively killed due to a researcher registering a hardcoded domain in the ransomware.

- It propagated through EternalBlue, an exploit for older Windows systems the DoublePulsar tool to install and execute a copies of itself. EternalBlue was stolen and leaked by a group called The Shadow Brokers a few months prior to the attack.

- The WannaCry ransomware epidemic appears to have ended as abruptly as it started, although not without first having infected +230,000 endpoints in more than 150 countries, many of them in the medical and manufacturing industries.

- The WannaCry outbreak also made extensive use of Equation Group tools, yet no one is suggesting that the Equation group is responsible for WannaCry, at least not directly.

- Careful planning appears to have gone into this event, including releasing the ransomware on a Friday, perhaps to increase chaos and response time for victims — a familiar tactic from other high-profile criminal attacks, such as the Bangladesh Bank crime. That the WannaCry variant was in more than 24 languages also suggests lofty goals for the criminals.

- The 97 transactions to the three hardcoded bitcoin addresses totaling approximately USD 25,000-, a very modest amount. Based on our research regarding ransomware payments, we’ve seen even a small-time operation earning approximately USD 100,000 over a few months.
Useful links:


Q & C?