Ransomware attacks or phishing e-mails are serious threats to companies. And no matter how well you may have secured your IT systems, an 'accident' is always around the corner. A moment of inattention on the part of an employee who clicks on the wrong link and enters his password there. Or hackers who have found an opening in a computer where the latest virus scanner has not been installed in time.
How to act if that is the case? This info sheet tells you which FIRST steps you should take. Hang it somewhere for all employees to see, so that even if the systems are down everyone knows how to act. Practice the emergency plan periodically as well.

THE TWO IMPORTANT STEPS IN A CYBER INCIDENT:
1. KEEP CALM
2. SEEK HELP AND CALL YOUR ICT SPECIALIST OR IT SERVICE PROVIDER (SEE LIST OF IMPORTANT TELEPHONE NUMBERS).

THERE ARE TWO MAJOR CYBER INCIDENTS, EACH OF WHICH REQUIRES ITS OWN APPROACH.

WHAT SHOULD I DO IN CASE OF A RANSOMWARE ATTACK?

1. DON'T PAY THE RANSOM
Paying never immediately solves the problem and encourages computer criminals to carry out more attacks.

2. DOCUMENT THE ATTACKER'S MESSAGE
Document messages from the attacker. Do you see a message on your screen? Note the date, time and activity and take a photo, screenshot or copy the message. This is also important for reporting to the police.

3. ISOLATE THE INFECTED COMPUTER(S) BY DISCONNECTING THEM FROM THE NETWORK
Prevent further spread of the infection across more devices. Isolate the infected computer(s) by disconnecting it from the network or turn off the Wi-Fi if you are working on a wireless network.
Note: Do not turn off the power unless you CANNOT unplug the devices. Without power, you may lose useful evidence.

4. REPORT THE INCIDENT AS SOON AS POSSIBLE, BOTH INTERNALLY AND EXTERNALLY
Inform relevant employees and managers and make sure they know what to look out for. You can also contact (by telephone) one or more of the authorities listed at the bottom of this information sheet.

Check (possibly with a third party or via computers that have not been connected to the network and cannot be infected) whether a key already exists to open the digital lock on No More Ransom.

You can put a computer in 'safe mode' with the help of third parties:
Windows **Apple**

See if you can remove the ransomware with the help of the free trial version of Sophos' HitmanPro program.

If there is a need, you can always contact the **Confidential Extortion Line (tel: 0800-2800 200)**, for entrepreneurs who are victims of threats or (digital) extortion. The Confidential Line lends an ear, and offers advice, support and a perspective for action.

VNO NCW MKB Nederland BouwendNederland

CYBER EMERGENCY PLAN
FIRST STEPS AFTER A CYBER ATTACK

WHAT SHOULD I DO IF I (OR AN EMPLOYEE) CLICKED ON A PHISHING E-MAIL?

1. DISCONNECT THE DEVICE FROM THE INTERNET
Find your Wi-Fi settings and disconnect from the network, or disconnect the internet cable from the affected device. This reduces the risk of malware spreading through the network.

2. CHANGE PASSWORDS
Did you / the employee end up on a fake website? Change the password! Is the password also in use for other accounts? Change these there too, preferably together with password hints and security questions.
Also have the administrator revoke all running sessions, as unauthorized persons may already be logged in with the password. If possible, perform a company-wide password reset to be extra careful.

3. REPORT THE INCIDENT AS SOON AS POSSIBLE BOTH INTERNALLY AND EXTERNALLY
Inform relevant personnel including managers and ensure they know what to look for. You can also contact one or more of the numbers below.
If necessary, carry out a virus scan with the help of an expert to have your computer checked for viruses and have them removed by the virus scanner. Always make sure you have downloaded the latest version of the virus scanner so that the latest threats are recognized.

WHERE CAN I GO AFTER A CYBER INCIDENT?

File a report with the **police**, online or at the nearest police station
Ph: 0800-8844

Report a data breach to the Dutch **Data Protection Authority**
Ph: 088-180 52 55

Report fraud to the **Fraudehelpdesk**
Ph: 088-786 73 72

Find general information at the **Digital Trust Center**

WRITE IMPORTANT OWN TELEPHONE NUMBERS HERE:

1. IT-department

2. IT-supplier

3. (cyber) insurer

4. (cyber) security specialist

5. .....

6. .....

7. .....