Orange
Cyberdefense

www.orangecyberdefense.com

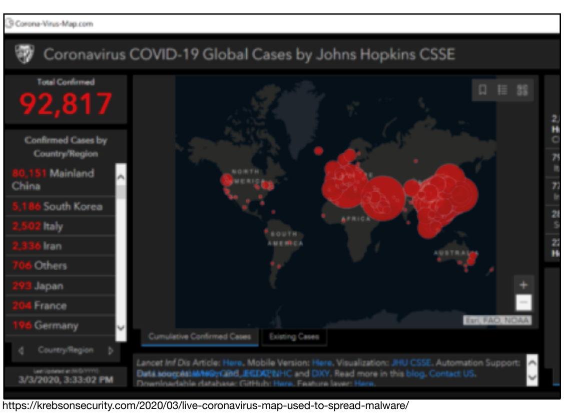
The cybersecurity risk intensifies along with COVID-19.

Theft of personal and banking information, leakage of confidential data, unavailability of systems essential for managing the health crisis... **There could be critical impacts.**

The pandemic we are currently facing is considerably **increasing cybersecurity risk:**

> **Malicious** actors exploit the global panic to spread **false information, malware and scams** of all kinds.
> The sudden shift to permanent **remote working** did not allow businesses to prepare for or mitigate possible **cyber attacks**.

Applications and malicious websites



Corona-Virus-Map.com

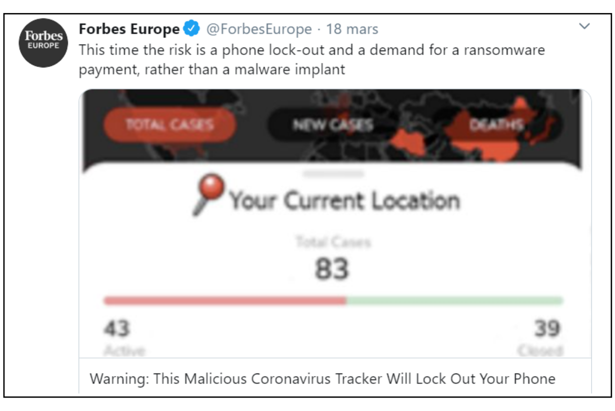
Coronavirus COVID-19 Global Cases by Johns Hopkins CSSE

Total Confirmed 92,817

Confirmed Cases by Country/Region

80,151 Mainland China
5,186 South Korea
2,502 Italy
2,336 Iran
706 Others
293 Japan
204 France
196 Germany

3/3/2020, 3:33:02 PM



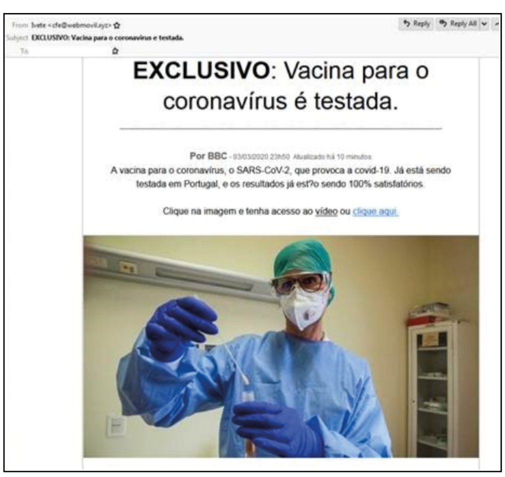
Forbes Europe @ForbesEurope · 18 mars
This time the risk is a phone lock-out and a demand for a ransomware payment, rather than a malware implant

Warning: This Malicious Coronavirus Tracker Will Lock Out Your Phone

https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/

This COVID-19 propagation map is based on a legit one, however, it contains a spyware that allows to recover passwords, bank card numbers or other **confidential data**. Other applications can lock phones and **demand a ransom**.

Phishing



From Ivete <cfe@webmovil.xyz>
Subject EXCLUSIVO: Vacina para o coronavirus e testada.
To

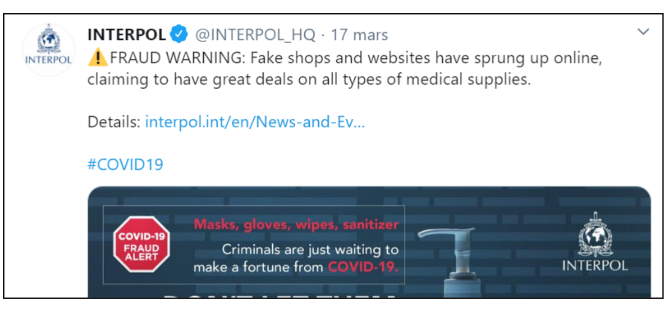
EXCLUSIVO: Vacina para o coronavírus é testada.

Por BBC - 03/03/2020 23h50 Atualizado há 10 minutos
A vacina para o coronavírus, o SARS-CoV-2, que provoca a covid-19. Já está sendo testada em Portugal, e os resultados já est?o sendo 100% satisfatórios.

Clique na imagem e tenha acesso ao vídeo ou clique aqui.

https://blog.f-secure.com/coronavirus-email-attacks-evolving-as-outbreak-spreads/

E-commerce fraud



INTERPOL @INTERPOL_HQ · 17 mars
⚠️FRAUD WARNING: Fake shops and websites have sprung up online, claiming to have great deals on all types of medical supplies.

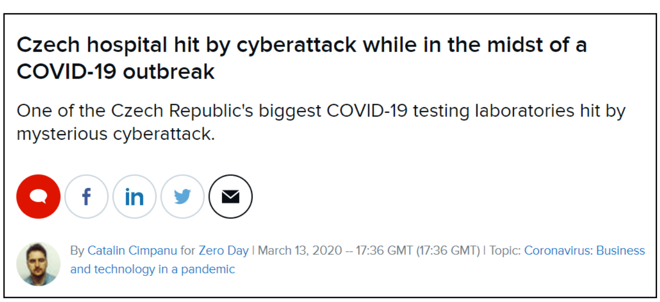
Details: interpol.int/en/News-and-Ev...

#COVID19

COVID-19 FRAUD ALERT
Masks, gloves, wipes, sanitizer
Criminals are just waiting to make a fortune from COVID-19.
INTERPOL

Be on high alert for scams: selling of masks, hydroalcoholic gel, miracle drugs or experimental vaccines, false calls for donations or other “fake news”.

The new targets: public and private healthcare organisations

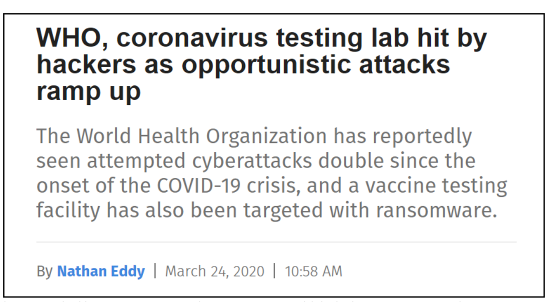


Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak

One of the Czech Republic's biggest COVID-19 testing laboratories hit by mysterious cyberattack.

By Catalin Cimpanu for Zero Day | March 13, 2020 -- 17:36 GMT (17:36 GMT) | Topic: Coronavirus: Business and technology in a pandemic

https://www.zdnet.https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/



WHO, coronavirus testing lab hit by hackers as opportunistic attacks ramp up

The World Health Organization has reportedly seen attempted cyberattacks double since the onset of the COVID-19 crisis, and a vaccine testing facility has also been targeted with ransomware.

By Nathan Eddy | March 24, 2020 | 10:58 AM

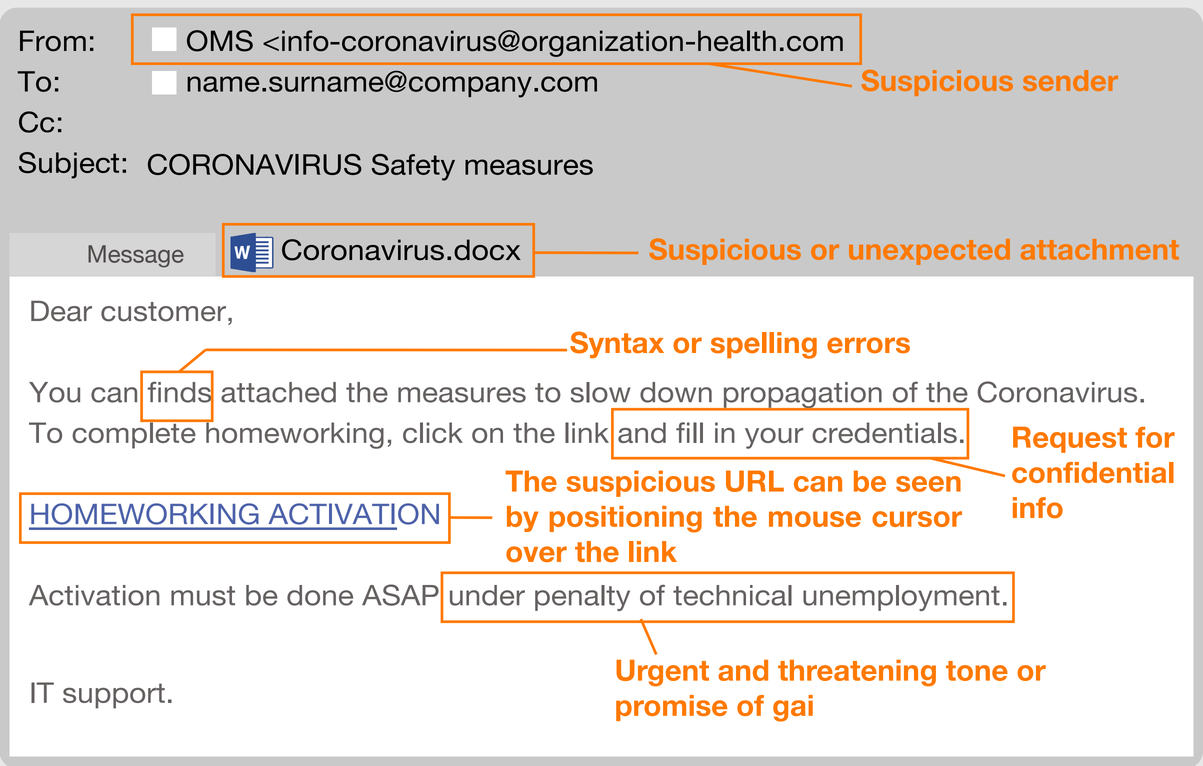
https://www.healthcareitnews.com/news/who-coronavirus-testing-lab-hit-hackers-opportunistic-attacks-ramp

Hackers remain agile: shortly after some governments implemented confinement exception permits, cyber criminals created malicious sites and rogue applications. These offered help to fill permits but in fact enable data theft and malware propagation. Be aware!

How to protect yourself and your organisation

Awareness against phishing

Phishing is a type of social engineering **attack**, aimed at stealing **confidential information** including login credentials and credit card numbers or to **install malware** on your computer.



From: OMS <info-coronavirus@organization-health.com
To: name.surname@company.com
Cc:
Subject: CORONAVIRUS Safety measures

Message | Coronavirus.docx

Dear customer,

You can finds attached the measures to slow down propagation of the Coronavirus.
To complete homeworking, click on the link and fill in your credentials.

HOMEWORKING ACTIVATION

Activation must be done ASAP under penalty of technical unemployment.

IT support.

Suspicious sender
Suspicious or unexpected attachment
Syntax or spelling errors
Request for confidential info
The suspicious URL can be seen by positioning the mouse cursor over the link
Urgent and threatening tone or promise of gai

Other elements can warn you of a phishing e-mail: an unusual subject, suspicious styling or layout, a non or poorly personalised e-mail, etc.

If you doubt if an e-mail is legitimate:

- 🚫 Don’t forward the e-mail to colleagues.
- 🚫 Don’t open the attachments, nor click on links.
- 🚫 Refuse to give passwords or confidential information (even to IT support).
- ○ Alert IT support immediately.

Our security tips for remote work:

Use a secure connection
Use the VPN to access the corporate network (via your internet box or phone). Avoid using public wifi networks, which may be hacked: your data may be intercepted and/or modified.

Separate professional and personal uses
Lock your computer to avoid unfortunate modifications or deletions. Those around you (e.g., children) should not use your workstation. Personal use must be restricted to limit the risks of hacking and overloading the corporate network.

Save your documents
Regularly save your documents on the corporate file server or corporate cloud storage to avoid data loss. Avoid using personal USB keys, which represent a significant vector of data leakage.

Ensure your equipment is protected
For homeworking as on company premises, remember to apply security updates and to use strong passwords: this could avoid an attack. Also, downloading software from the internet creates some dangers. Contact your IT department if you need new software or applications.

Be vigilant when browsing the internet
Internet browsing can expose you to malware. It can infect your computer when visiting websites that have been hacked, those that are unsafe or illicit (games, counterfeits, downloads). Be aware of these risks.

Does your workstation behave abnormally?
Do you think you have clicked on a phishing e-mail?
In case of doubt, contact your IT Security Team.