CYBER*AWARE*

Are you Cyber Aware?

In the news

Cyber attack sweeps globe, researchers see 'WannaCry' link

Cybercrime

Petya ransomware attack: what is it and how can it be stopped?

Companies have been crippled by an attack dubbed 'Petya', the second major ransomware crime in two months. **Olivia Solon** answers the key questions
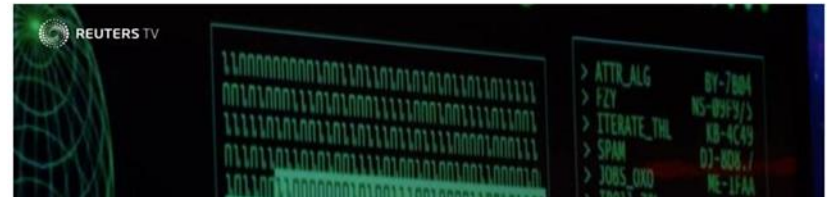
Olivia Solon in San Francisco

@oliviasolon

email

Wednesday 28 June 2017 07.17 BST

Petya cyber attack: What's going on with the latest ransomware virus?

By Jessica Haynes

Updated 55 minutes ago

A massive ransomware attack has hit computers and servers across the globe causing turmoil in its path.

European Commission

The corporate awareness programme

CYBER*AWARE*

Priority messages

Take active measures to ensure **safe** use of ICT services onsite and offsite.

Browse and download safe - CheckSource, Https

Be aware of suspicious e-mails - phishing is a real problem

Secure your password - 12345 a comic option, isn't it?

Store and transfer safe - BackUp

Share safe - Encryption, DataProtection

4

1. Check source

CYBER*AWARE*

BROWSE & DOWNLOAD SAFE
NEVER SURF THE INTERNET
IF YOU HAVE ADMINISTRATOR
RIGHTS.
INSTALL SOFTWARE ONLY
FROM REPUTABLE SOURCES.

Be Cyber Aware, use https

https://cybersecuritymonth.eu/

2. Suspicious e-mails

PHISHING
BE CAREFUL
WHEN OPENING
A FRIENDLY EMAIL
FROM A STRANGER

IF YOUR COMPUTER IS ATTACKED,
IT CAN COMPROMISE YOUR COLLEAGUES' WORK

Spear Phishing!

- The spear phisher thrives on familiarity. He has your email, knows your name, and at least a little about you.

- They might scan social networking sites, conference sites, your posts telling friends about a cool new gadget bought online, tweets about news…

8

Be Cyber Aware!

1. Separate your work & social identity

2. Report the spam/phishing mail

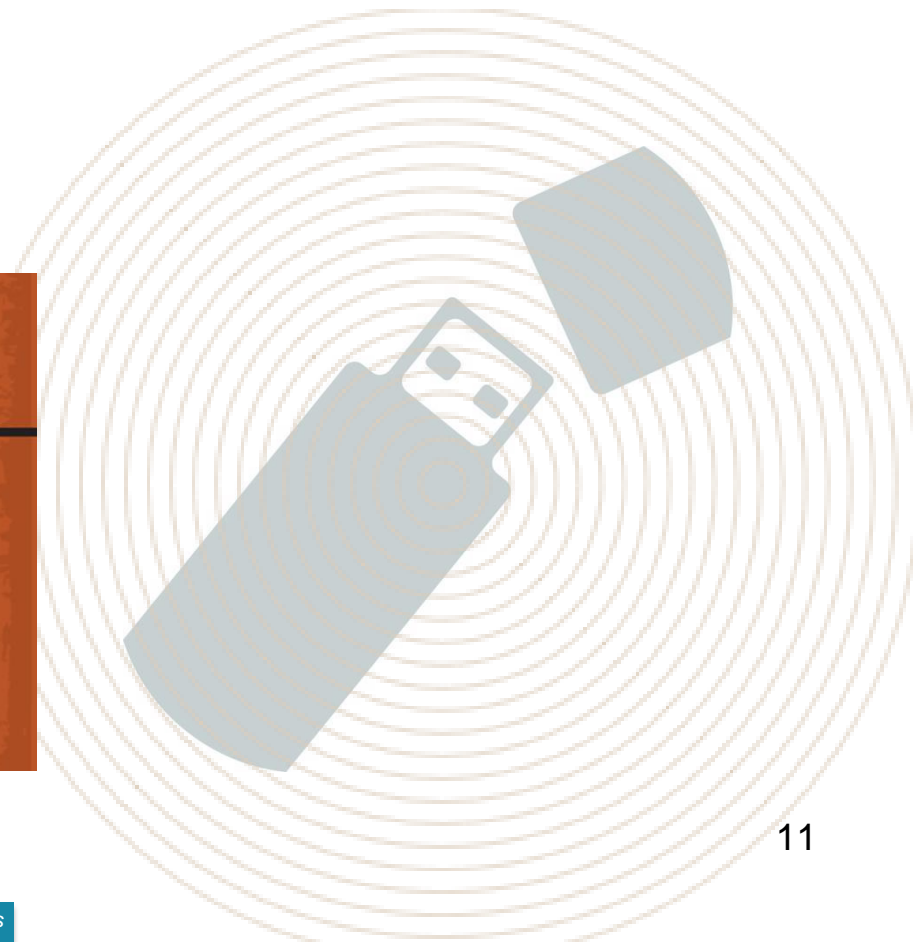3. If you clicked on the link, report it

3. Secure your password

CYBER*AWARE*

SECURE
YOUR PASSWORD
PASSWORDS ARE PERSONAL,
KEEP THEM SECRET

4. Store and transfer safe

CYBER*AWARE*

STORE
& TRANSFER
SAFE

DON'T USE USB STICKS
FROM UNKNOWN ORIGIN

5. Share safe

CYBER*AWARE*

SHARE SAFE

DON'T SHARE PRIVATE DATA
IN PUBLIC NETWORKS.
DON'T LEND CORPORATE
DEVICES TO FAMILY
AND FRIENDS

12

Cyber Aware
Tip #1 :
Connect only
when needed

Always turn off Wi-Fi,
location services and
Bluetooth when not in
use

Save your battery!

13

Cyber Aware Tip #2: apps for mobile

- **Only install apps from official app stores**
- Before downloading an app, research the app and its publishers.
- Be cautious of links you receive in email and text messages that might trick you into installing apps from third party or unknown sources.
- Check other users' review and ratings
- Read the app's permissions
- Install a mobile security app

Shut down the device when you go for patching and updating your system.

Cyber Aware Tip #3: PC shut down

15

Lock your screen when away in order to protect your information and avoid third party direct access.

Cyber Aware Tip #4: Lock screen

Be Cyber Aware!

Understand Cyber Security

Train and **update** yourself with available

resources: videos, articles, information

sessions, anti-phishing exercise, classroom

training, e-learning…

17

"We all need to adopt **#safe** cyber skills and promote a **#cyberawareness** culture, at work and in our private lives"

Mariya GABRIEL
EU Commissioner
Digital Economy & Society

We aim to make every Commission staff member #CyberAware

European Commission

European Commission

Other resources

- [European Cyber Security Month](#)
- [NIS quiz](#)
- [NIS educational map](#)
- European cyber security [challenge](#)

and posters in many EU languages

https://www.enisa.europa.eu/media/multimedia/posters/cybersecurity-education-posters-2016

European Commission