



PT LAB

Jak moc pomáháme útočníkům s přípravou útoku proti nám samým? Aktuální hrozby v oblasti kybernetické bezpečnosti

*David Malaník*

PT LAB – Penetration Testing Laboratory  
Fakulta aplikované informatiky  
Univerzita Tomáše Bati ve Zlíně  
E-mail: [dmalanik@utb.cz](mailto:dmalanik@utb.cz)



# Stručný itinerář

---

Co považujete za moderní technologie?

---

BYOD

---

Bezdrátové technologie

---

Informace = zbraň

---

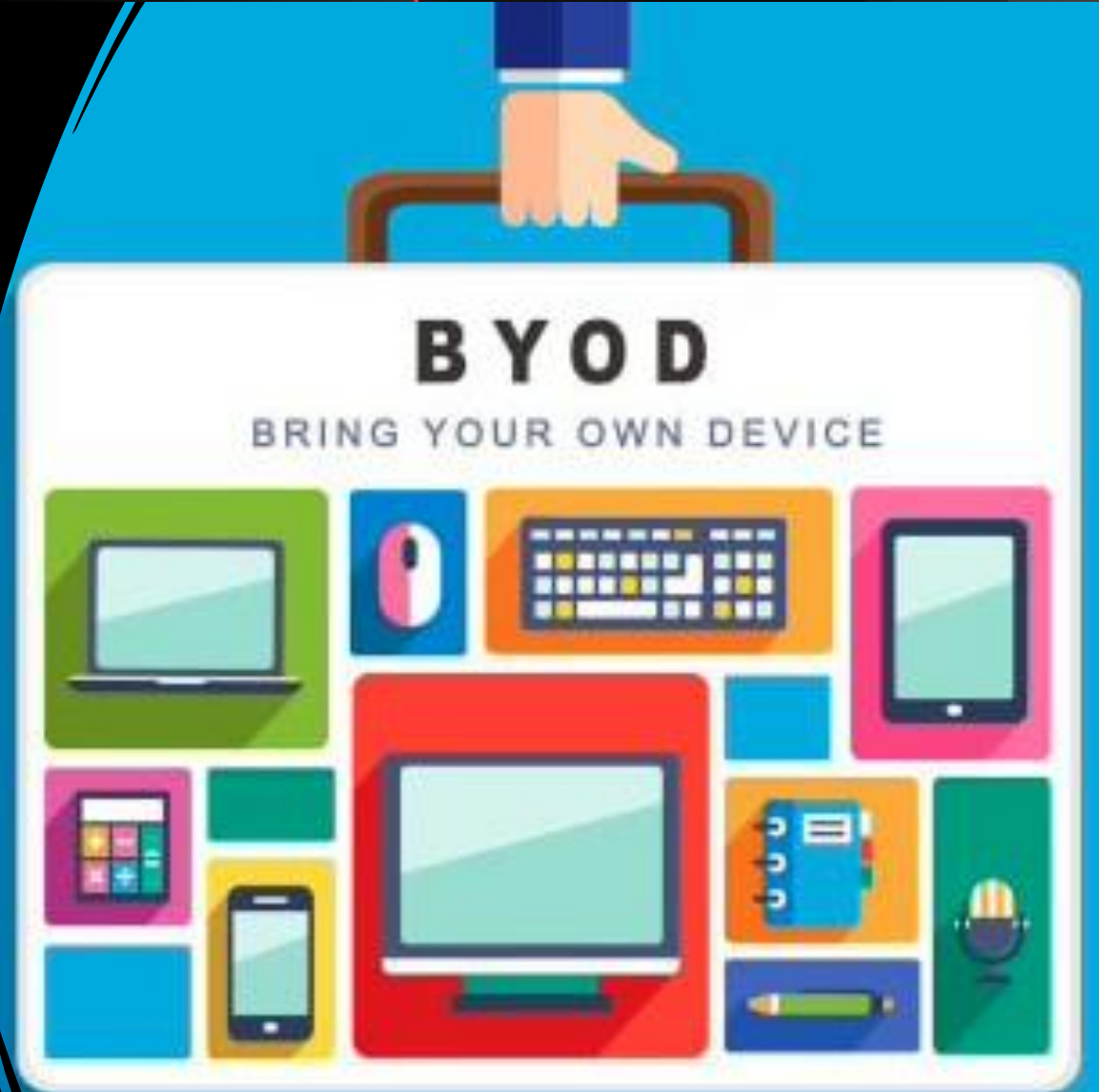
AI?

---

Jak se bránit?

# BYOD

- **B**ring **Y**our **O**wn **D**evice
- **B**reak **Y**our **O**wn **D**atacenter
- **B**roadcast **Y**our **O**wn **D**ata
- Trend / Home Office



# BYOD

- Cíl je jasný -> ušetřit/ulehčit (ale komu ?)
  - Každý máme spoustu vlastní techniky
  - Proč bych musel hlídat nabíjení ... a další
- Skloubit využití osobních zařízení s prací ?
  - Ušetříme ... ? Opravdu ... ?
  - Proč se může jednat o problém ?

# BYOD

- Scénáře
  - Osobní zařízení ve firemní síti
  - Osobní zařízení na práci vzdáleně
    - S připojením/bez připojení
- Firemní zařízení doma ?
- Sdílené zařízení ?
  - „Poděděné zařízení“
  - „Rozděl a panuj“
  - „Vymazat .. Bezpečně“



PT LAB

# Bezdrátové technologie



## Dostupnost sítí

Veřejné sítě  
Hot-spoty  
Firemní sítě



## Zabezpečení

Heslo  
Login + Heslo  
Certifikát  
Skryté sítě



## Jste na Wi-Fi?

Připojili jste se na nějakou  
Wi-Fi zde?  
Znáte tu síť?



## Jak jste se na ni dostali?

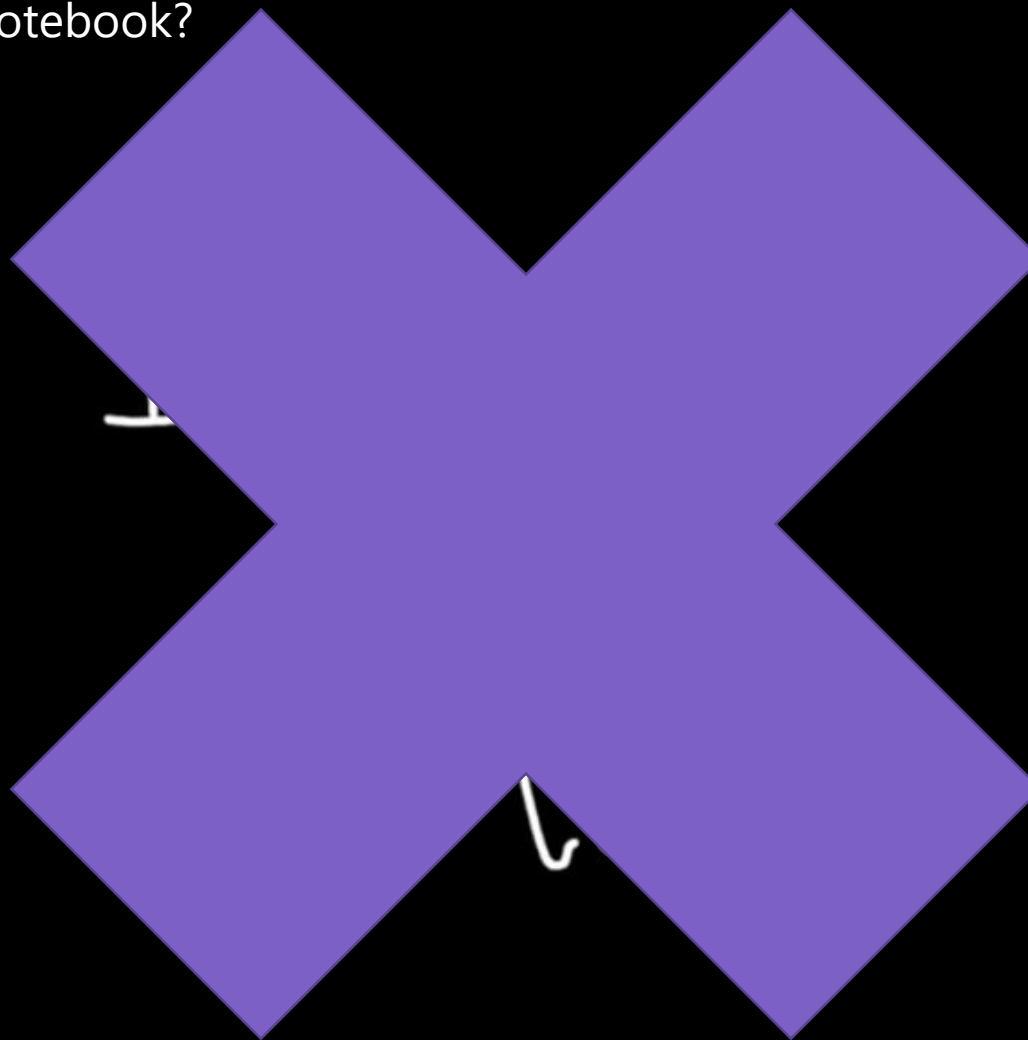
Otevřená síť  
Lísteček na stole  
Jinak



PT LAB

# Tak se na to podívejme prakticky

Vypínáte si telefon nebo notebook?





# Co lze získat?

- Pokud jste se připojili (bez VPN) tak je vidět:
  - Jednoznačný identifikátor Vašeho zařízení
  - Název sítě do které se připojujete -> <https://www.wigle.net>
  - Služby, které používáte
  - Možná i nějaké heslo....
  - INFORMACE!

10.0.25.67	255.255.255.255	DB-LSP-DISC/JSON	209 Dropbox LAN sync Discovery Protocol, JavaScript Object Notation
10.0.25.67	10.0.25.255	DB-LSP-DISC/JSON	209 Dropbox LAN sync Discovery Protocol, JavaScript Object Notation

```
Additional RRs: 7
v Answers
  v jiří - MacBook Pro (3)._device-info._tcp.local: type TXT, class IN
    Name: ██████████ MacBook Pro (3)._device-info._tcp.local
    Type: TXT (Text strings) (16)
    .000 0000 0000 0001 = Class: IN (0x0001)
    0... .... .... .... = Cache flush: False
    Time to live: 4500 (1 hour, 15 minutes)
    Data length: 51
    TXT Length: 20
    TXT: model=MacBookPro14,2
    TXT Length: 10
    TXT: osxvers=22
    TXT Length: 18
    TXT: ecolorm=157,157,160
  > companion-link._tcp.local: type PTR, class IN, ██████████ MacBook Pro (3).companion-link._tcp.local
```



# Informace = zbraň !!!



## Citlivá informace?

IP/FQDN?

Jméno?

Vaše firemní síť?

Vaše domácí síť?

Vaše hesla?



## Profilování

Internet je dokonale persistentní zdroj dat –  
problematika vymazání dat

Veřejné zdroje informací

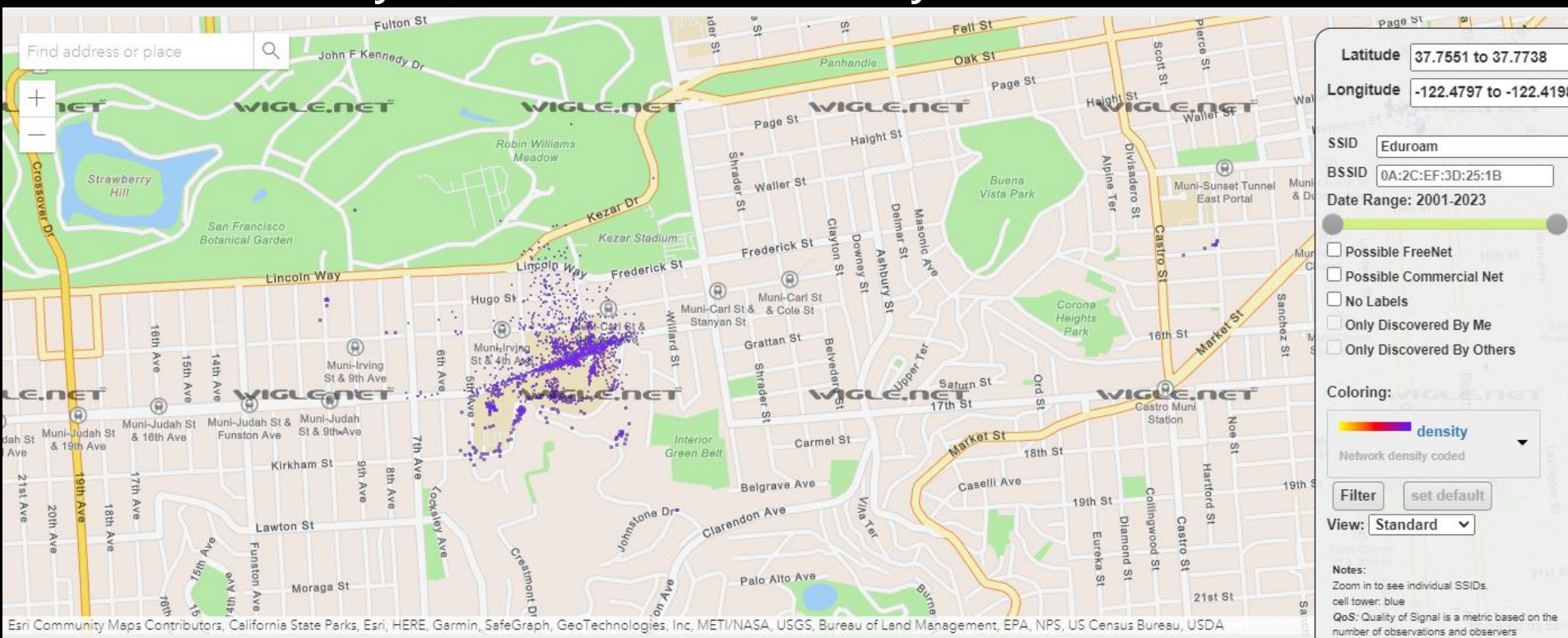
Pasivní sběr informací o našich technologiích

Aktivní sběr např. Wi-Fi, IMSI catcher.



## Informace = zbraň – ukázky

- Databáze Wi-Fi
  - <https://www.wigle.net/>
  - Databáze známých Wi-Fi sítí dle lokality



# Informace = zbraň – ukázky

- Registr smluv I
  - <https://smlouvy.gov.cz/smlouva/8373015?backlink=ew55v>

Doručovací adresa Realizátora projektu:

**Česká agentura na podporu obchodu/CzechTrade**

k rukám: Ing. Eva Novotná  
adresa: Dittrichova 21, Praha 2, PSČ 128 01  
e-mail: [eva.novotna@czechtrade.cz](mailto:eva.novotna@czechtrade.cz)  
Datová schránka: afrv7v6

Doručovací adresa Příjemce podpory:

**Elektrotechnická asociace ČR**

k rukám: Ladislav Sojka  
adresa: [Zelený pruh 95/97](#), 140 00, Praha 4 - Braník  
e-mail: [sojka@electroindustry.cz](mailto:sojka@electroindustry.cz)  
Datová schránka: w463txn



## Informace = zbraň – ukázky

- Registr smluv III – může být i hůř

Ing. Michal Laštovka

Digitálně podepsal Ing. Michal Laštovka  
 DN: c=CZ, 2.5.4.97=NTRCZ-66002222, o=Česká republika, Ministerstvo pro místní rozvoj, ou=Ministerstvo pro místní rozvoj ČR, ou=4642, cn=Ing. Michal Laštovka, sn=Laštovka, givenName=Michal, serialNumber=P556995, title=VORS  
 Datum: 2022.11.01 21:40:46 +01'00'

Česká republika - Ministerstvo pro místní rozvoj

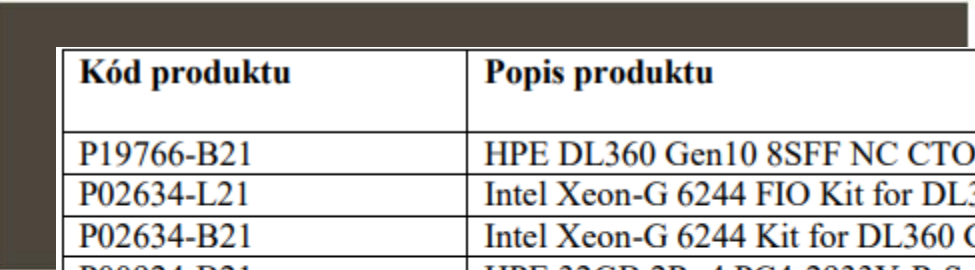


, vedoucí Oddělení realizace MS

Ing. Subhi Brož, Ph.D.

Digitálně podepsal Ing. Subhi Brož, Ph.D.  
 Datum: 2022.11.01 17:14:49 +01'00'


C SYSTEM CZ a.s.



Kód produktu	Popis produktu	Počet ks
P19766-B21	HPE DL360 Gen10 8SFF NC CTO Svr	2
P02634-L21	Intel Xeon-G 6244 FIO Kit for DL360 G10	2
P02634-B21	Intel Xeon-G 6244 Kit for DL360 Gen10	2
P00924-B21	HPE 32GB 2Rx4 PC4-2933Y-R Smart Kit	32
P21131-B21	HPE 800GB SAS MU SFF SC SS540 SSD	4
867982-B21	HPE DL360 Gen10 LP Riser Kit	2
867328-B21	HPE 10/25GbE 2p SFP28 QL41401 Adptr	2
867334-B21	HPE 10/25GbE 2p FLR-SFP28 QL41401L CNA	2

## Informace = zbraň – ukázky

- Registr smluv IV – může být i hůře



2

mailto:helpdesk@pragodata.com

7. Zhotovitel pro určené zástupce objednatele zprovozní dostupný minimálně v pracovní dny době od 07:00 do
8. Kontakt pro hlášení požadavků HelpDesk/ ServiceDes
  - e-mail: [\[redacted\]](#)
  - telefon: +420 [\[redacted\]](#)
  - adresa pro přihlášení: [\[redacted\]](#)

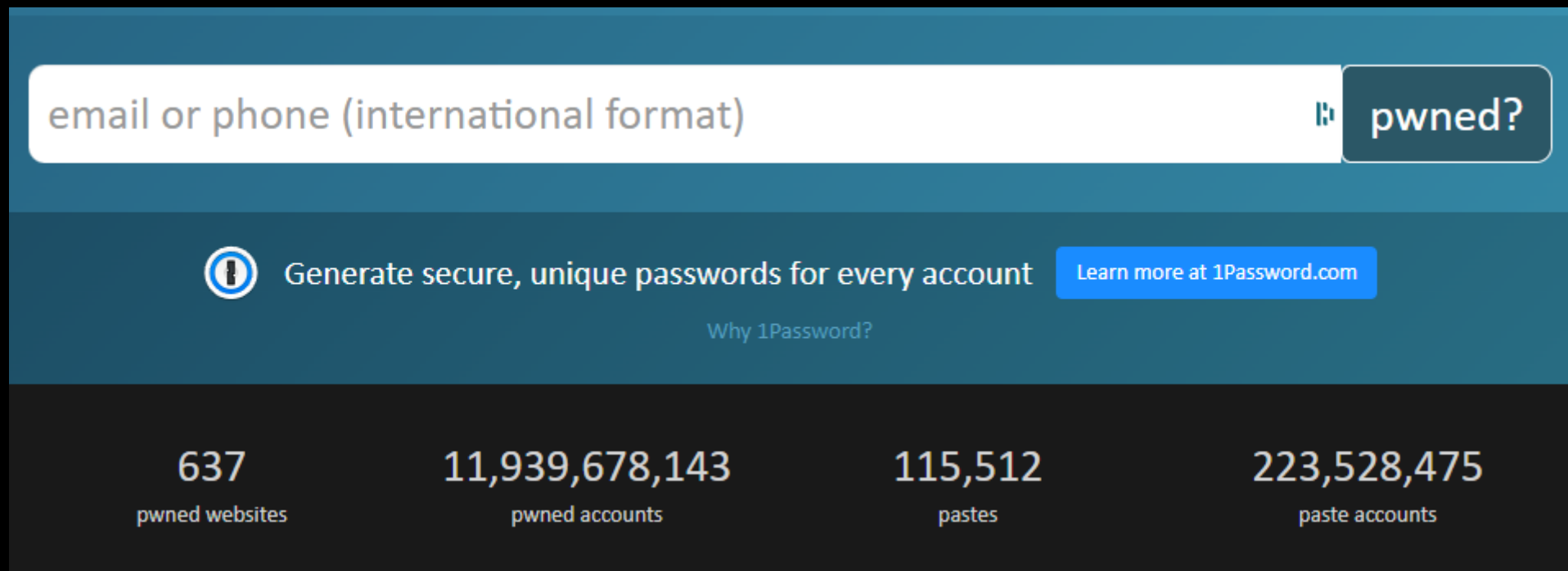
### III.

#### Práva a povinnosti objednatele


1. Objednatel se zavazuje, že zhotoviteli za realizaci díla a posky s touho smlouvou uhradí odměnu dle dalších ustanovení této
2. Objednatel se zavazuje poskytnout zhotoviteli při plnění te součinnost sám nebo na výzvu zhotovitele.

# Informace = zbraň – ukázky

- HIBP
  - <https://haveibeenpwned.com/>
  - Veřejná DB na hledání uniklých loginů



email or phone (international format) **pwned?**

 Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

[Why 1Password?](#)

637	11,939,678,143	115,512	223,528,475
pwned websites	pwned accounts	pastes	paste accounts



PT LAB

# Informace = zbraň – ukázky

- Firemní emaily



**Cristian Sánchez**

*Grant Holder Manager*

*DigForASP - CA17124*

**Departamento de Matemáticas**

**Universidad de Cádiz**

**Facultad de Ciencias, Campus del Río San Pedro**

**11510 Puerto Real**

**Cádiz - SPAIN**

**Tel +34 956 012 703**

**[www.uca.es](http://www.uca.es)**





# Informace = zbraň – ukázky

- Domény

Výběr domén *				
<input type="checkbox"/>	cacio.cz	obsazená		
<input type="checkbox"/>	cacio.eu	obsazená		
<input checked="" type="checkbox"/>	cacio.online	registrovat doménu	1 rok	<del>800.00 Kč</del> 99.00 Kč
<input type="checkbox"/>	cacio.com	obsazená		
<input type="checkbox"/>	cacio.net	obsazená		
<input type="checkbox"/>	cacio.store	obsazená		

Doporučené domény				
<input type="checkbox"/>	cacio.sk	registrovat doménu	1 rok	<del>265.00 Kč</del> 150.00 Kč
<input type="checkbox"/>	cacio.pl	registrovat doménu	1 rok	99.00 Kč
<input type="checkbox"/>	cacio.cloud	registrovat doménu	1 rok	<del>340.00 Kč</del> 22.00 Kč
<input type="checkbox"/>	cacio.site	registrovat doménu	1 rok	<del>598.00 Kč</del> 0.00 Kč
<input type="checkbox"/>	cacio.tech	registrovat doménu	1 rok	<del>1,359.00 Kč</del> 119.00 Kč
<input type="checkbox"/>	cacio.info	registrovat doménu	1 rok	<del>400.00 Kč</del> 175.00 Kč

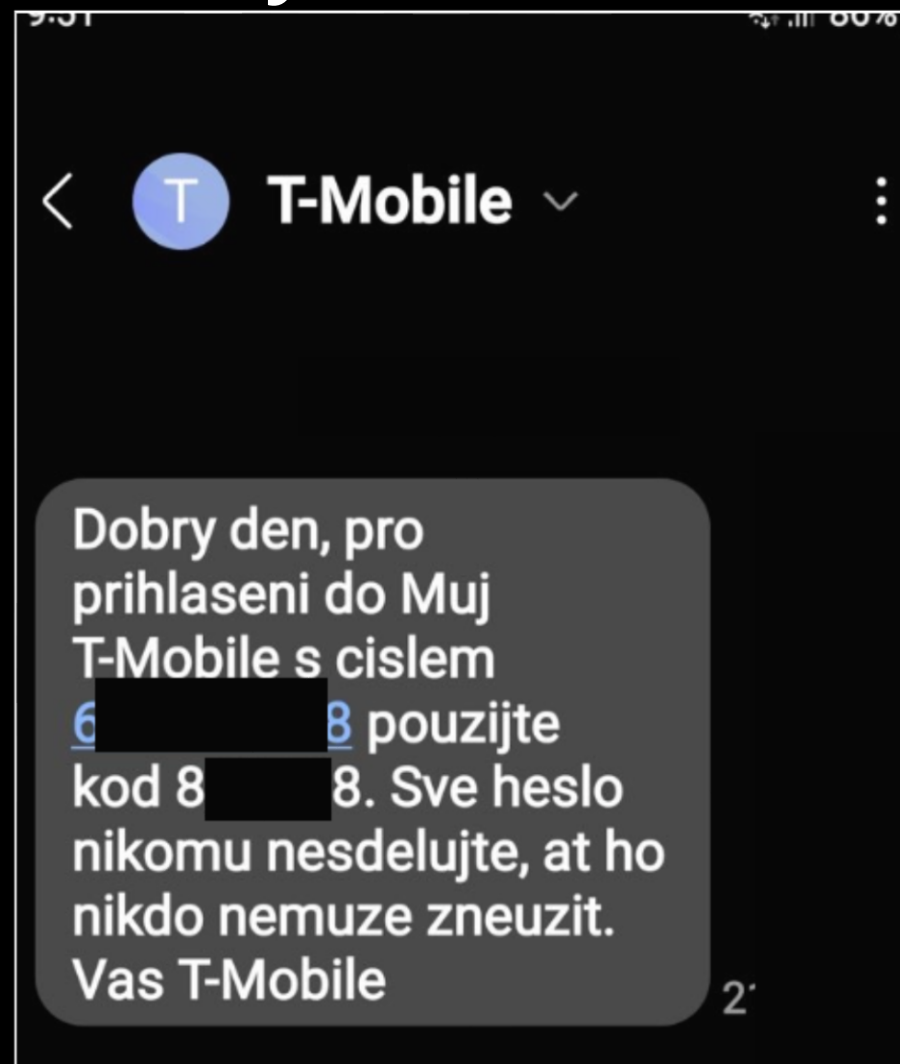
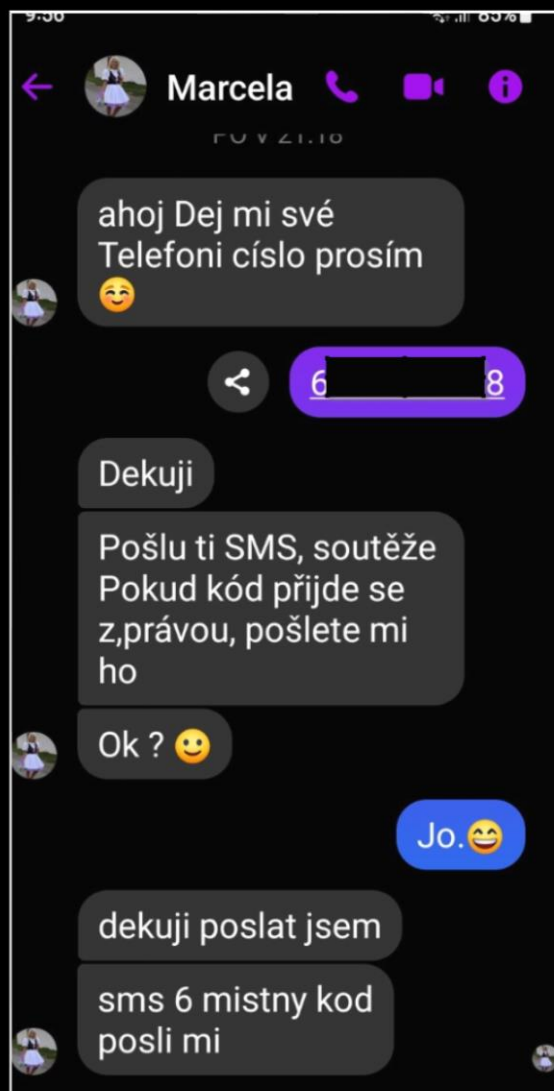
K F-Page 1. rok zdarma





# Informace = zbraň – ukázky

- social

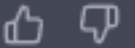




AI?



Sure, here's a Python code that generates random passphrases of length 8 to 12 using the characters 'a'-'z', 'A'-'Z', and '0'-'9':



python

Copy code

```
import random
import string

def generate_passphrase(length):
    """Generate a passphrase with the given length."""
    chars = string.ascii_letters + string.digits
    return ''.join(random.choice(chars) for _ in range(length))

for i in range(8, 13):
    passphrase = generate_passphrase(i)
    print(passphrase)
```



# AI?

AL

default password for HP ilo



The default password for HP iLO (Integrated Lights-Out) is "admin". However, for security reasons, it is recommended that you change the default password after the initial setup.



If the default password has been changed and you have lost or forgotten the new password, you can reset the iLO to factory defaults. This can be done through the iLO web interface or by pressing the iLO reset button on the server's motherboard. However, resetting to factory defaults will erase any settings and configurations that have been made on the iLO, so it should only be used as a last resort.



# AI?



Here's a Python code that generates all possible passphrases of length 8 to 12 using the characters 'a'-'z', 'A'-'Z', and '0'-'9' and ensures that each passphrase has at least 2 uppercase letters and 2 numbers:

python

Copy code

```
import itertools
import string

def generate_passphrases():
    """Generate all possible passphrases with the given constraints."""
    chars = string.ascii_lowercase
    uppercase_chars = string.ascii_uppercase
    digits = string.digits
    for length in range(8, 13):
        for uppercase_positions in itertools.combinations(range(length), 2):
            for digit_positions in itertools.combinations(range(length), 2):
                for uppercase_combinations in itertools.combinations(uppercase_chars, 2):
                    for digit_combinations in itertools.combinations(digits, 2):
                        passphrase = [random.choice(uppercase_combinations) if i in uppercase_positions else
                                      random.choice(chars) if i in digit_positions else
                                      random.choice(digits) if i in digit_combinations else
                                      random.choice(chars) for i in range(length)]
                        yield ''.join(passphrase)

for passphrase in generate_passphrases():
    print(passphrase)
```

7Hdgu3pv

8Hzew8if

3Vghs3xo

5Hcoo5pv

6Hyxh6ai

4Vc7n7mh

4Vyxg8iq

9Vbxh9ag

5Vemj5ig

5Hbib5oc

# Jak se bránit?

- Být paranoidní
  - Aspoň trochu....
- Izolace domácích zařízení a firemních – obzvláště na kritických postech
- Zabezpečení přenosných zařízení:
  - Šifrování
  - VPN připojení – required!
  - Zamykání zařízení
  - Vzdálený přístup + monitoring zařízení – možnost vzdáleného smazání.
- Opatrnost se zveřejňováním informací...



## Jak se bránit? (když útočíte)

61	0.830650494	192.168.0.141	172.64.153.207	QUIC	1399	Initial, DCID=1e9c8cc702eb9d56, SCID=7f5956, PKN: 0, CRYPTO
62	0.843199491	172.64.153.207	192.168.0.141	QUIC	1242	Initial, DCID=7f5956, SCID=015a347d482c5ff4be5a2b7ddd2c73f18da2f9f0, PKN: 0, A
63	0.845029656	172.64.153.207	192.168.0.141	QUIC	1242	Initial, DCID=7f5956, SCID=015a347d482c5ff4be5a2b7ddd2c73f18da2f9f0, PKN: 1, C
64	0.845136870	172.64.153.207	192.168.0.141	QUIC	1242	Handshake, DCID=7f5956, SCID=015a347d482c5ff4be5a2b7ddd2c73f18da2f9f0
69	0.847968836	192.168.0.141	172.64.153.207	QUIC	116	Protected Payload (KP0), DCID=015a347d482c5ff4be5a2b7ddd2c73f18da2f9f0
70	0.848028376	192.168.0.141	172.64.153.207	TLSv1...	105	Application Data
71	0.848228436	192.168.0.141	172.64.153.207	TLSv1...	90	Application Data
72	0.848241763	192.168.0.141	172.64.153.207	TCP	66	60644 → 443 [FIN, ACK] Seq=1328 Ack=15482 Win=64128 Len=0 TSval=2502093098 TSecr=2502093098
73	0.859704497	172.64.153.207	192.168.0.141	TCP	66	443 → 60644 [ACK] Seq=15482 Ack=1304 Win=65536 Len=0 TSval=1690142311 TSecr=2502093098

```

> Frame 69: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface
> Ethernet II, Src: PcsCompu_d4:c0:c5 (08:00:27:d4:c0:c5), Dst: Tp-LinkT_d3:ac:c5
> Internet Protocol Version 4, Src: 192.168.0.141, Dst: 172.64.153.207
> User Datagram Protocol, Src Port: 42652, Dst Port: 443

```

```

< QUIC IETF
  > QUIC Connection information
    [Packet Length: 74]
  > QUIC Short Header DCID=015a347d482c5ff4be5a2b7ddd2c73f18da2f9f0
  < [Expert Info (Warning/Decryption): Failed to create decryption context: Secrets are not available]
    [Failed to create decryption context: Secrets are not available]
    [Severity level: Warning]
    [Group: Decryption]
  Remaining Payload: 43b0210fc0ea11163cd503602aca3825ed5978ce1a82497fc6f4d72d...

```

```

0000 ac 84 c6 d3 ac cb 08 00 27 d4 c0 c5 08 00 45 00 ..... '.....E.
0010 00 66 00 00 40 00 40 11 33 42 c0 a8 00 8d ac 40 .f..@.@.3B....@
0020 99 cf a6 9c 01 bb 00 52 07 a9 56 01 5a 34 7d 48 .....R..V.Z4}H
0030 2c 5f f4 be 5a 2b 7d dd 2c 73 f1 8d a2 f9 f0 43 ,_·Z+}·,s.....C
0040 b0 21 0f c0 ea 11 16 3c d5 03 60 2a ca 38 25 ed .!.....<..*·8%·
0050 59 78 ce 1a 82 49 7f c6 f4 d7 2d e6 f0 8e 4b ba Yx··I····-··K·
0060 8d 1d 57 5d 84 33 6a ef a5 bc 95 4a 8b 55 1a 18 ··W]·3j····J·U·
0070 7c 2b e6 26 |+·&

```

```

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Compression Methods Length: 1
> Compression Methods (1 method)

```

```

00e0 00 02 40 01 00 39 00 53 01 04 80 00 75 30 09 01 ..@..9·S.....u0..
00f0 10 80 ff 73 db 0c 00 00 00 01 da 9a 5a da 00 00 ...s.....Z...
0100 00 01 04 04 81 80 00 00 6a b2 00 c0 00 00 00 ff .....j.....
0110 02 de 1a 02 43 e8 0e 01 08 06 04 80 10 00 00 08 .....C.....
0120 01 10 0f 03 7f 59 56 07 04 80 10 00 00 0b 01 14 .....YV.....
0130 20 01 00 05 04 80 c0 00 00 0c 00 00 15 00 c5 00 .....
0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```



PT LAB

# PENETRATION TESTING LABORATORY

<http://ptlab.fai.utb.cz>



Příležitost k dotazům



PT LAB

# PENETRATION TESTING LABORATORY

<http://ptlab.fai.utb.cz>



Heslo wifi: zlatihvezda.cz





PT LAB

# PENETRATION TESTING LABORATORY

<http://ptlab.fai.utb.cz>

