LABORATÓRIO DE INSTRUMENTAÇÃO
E FÍSICA EXPERIMENTAL DE PARTÍCULAS
partículas e tecnologia

Best practices for end-users in IT

Nuno Dias

~~*Insecure by nature*~~

1.
Electronic Mail

Or Email

Electronic Mail

From: Good_Intentions@hell.hot
To: 1_Person, ~~20_Persons~~
CC: Several_Persons
Subject: This is very Important

- "Good vs Bad" Forward
- Lists in To:
- Disclose internal Emails to outside

Electronic Mail

SPAM

- Forward all mail
- SPAMLEARN

Electronic Mail

SPAM

- Phishing
- Ransomware

Electronic Mail

SPAM

- ✔ **Phishing**
- ✔ **Ransomware**

From: DHL Global Mail Inc © <info3@s171003.smrtp.ru>
Reply-To: DHL Notification Team© <pt.autoreply@dhl-supply.com>, DHL Notification Team© <pt.autoreply@dhl-supply.com>
To: Delivery Team <dhlofficial@customer.com>
Subject: DHL- Seu pacote chegou, mas com problemas. - Urgente
Date: Wed, 20 Feb 2019 14:52:09 +0000

Caro info,

Eu cheguei com sua remessa. Mas eu sou incapaz de alcançar você.
Não consigo localizar o endereço físico final na carta de porte aéreo para essa entrega.

Por favor, encontre o seu formulário de contato. Também anexei a fatura comercial que recebi para isso.

Anexei meu número de telefone pessoal também para facilitar o contato.

Por favor, verifique o arquivo e confirme os detalhes.

Aguardo sua gentil resposta. Urgente.

Atenciosamente,

Gzip archive attachment (DHL AWB TRACKING DETAILS_pdf.gz)

From: EMS PARCEL INTERNATIONAL via Irtf <[redacted]>
Reply-To: EMS PARCEL INTERNATIONAL <csu@emsng.com>, Incider
To: Recipients <csu@emsng.com>
Subject: [Irtf] Shipment Document Arrival Notification
Date: Tue, 26 Feb 2019 00:19:28 -0800 (*26/02/19 08:19:28*)

Dear Customer

We are sending the shipping invoice as attached.
Packing information is as follows;

One case
22x33x23 cm, 1.6Kg

Best Regards,

∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞
Ryousuke Numata (Mr.)

Sales Department
Overseas sales Division

EMS Unit
Universal Postal Union
International Bureau
PO Box 312
3000 BERNE 15
1-1-62, Nakane, Soka,
Saitama, 340-0005,JAPAN
Tel: 81-48-933-1582
Fax: 81-48-933-1591

柴田科学株式会社
営業部海外課
沼田　亮介
〒340-0005 埼玉県草加市中根１-１-６２
tel : 048-933-1582 FAX. : 048-933-1591
カスタマーサポートセンター（製品の技術的サポート専用）
フリーダイヤル0120-228-766
∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞∞

ACE archive attachment (Ems invoice.ace)

Electronic Mail

SPAM

- ✔ **Phishing**
- ✔ **Ransomware**

From: Banco santander <no-reply@santander.pt>
To: Recipients <no-reply@santander.pt>
Subject: Atualizações bancárias on-line
Date: Tue, 19 Feb 2019 09:10:28 +0100 (*19/02/19 08:10:28*)

Estimado cliente

Actividades Incomuns foram detectadas na sua conta online Banco Santander, colocamos sob restrição. Para recuperar sua conta Clique Aqui para atualizar e verificar suas informações agora.

Saudações,
Unidade de Prevenção de Fraudes,
© 2019 Banco Santander, S.A

From: info@lip.pt
To: info@lip.pt
Subject: FWD: Comunicado Importante Itau Empresas 22/02/2019 03:16:42
Date: Fri, 22 Feb 2019 15:16:42 +0000 (GMT)

Atencao - Comunicado Importante Itau Empresas N°: 577856063 Prezado Cliente Itau: info@lip.pt

comunicação digital itaú

Prezado(a) Cliente Pessoa Juridica:

Lembramos você que em nosso sistema ainda não consta a sincroni- zação de seu **iToken / iToken no aplicativo.**

O seu prazo para sincronização foi prorrogado e deverá ser efetuado até o dia **22/02/2019**.

Evite o bloqueio do acesso **ONLINE** da sua conta na Internet e também do acesso nos **Caixas eletrônicos Itaú** fazendo agora mesmo a Sincronia Semestral.

Clique no link abaixo para iniciar:

Clique Aqui

Atenciosamente,
Banco Itaú

Itaú feito para você

O Banco Itaú garante o sigilo dos seus dados. Acesse o site do Banco Itaú e conheça a nossa política de privacidade. Por favor, não retorne este e-mail. Para nos contatar utilize o Fale Conosco do site do Banco Itaú.

Dúvidas, reclamações e sugestões, na sua agência. Se for necessário, utilize: SAC Itaú todos os dias, 24h 0800 728 0728. Fale Conosco www.itau.com.br . Se não ficar satisfeito com a solução apresentada, utilize: Ouvidoria Corporativa Itaú 0800 570 0011 dias úteis das 9 às 18h, Caixa Postal nº 67.600 - CEP 03162-971. Deficiente auditivo todos os dias 24h 0800 722 1722.

O seu e-mail está cadastrado para receber este tipo de mensagem do Banco Itaú. Para ALTERAR suas preferências ou CANCELAR o recebimento deste tipo de e-mail, acesse o seu Itaú Bankline Empresa na rota Produtos e Serviços > Comunicação Digital Itaú.

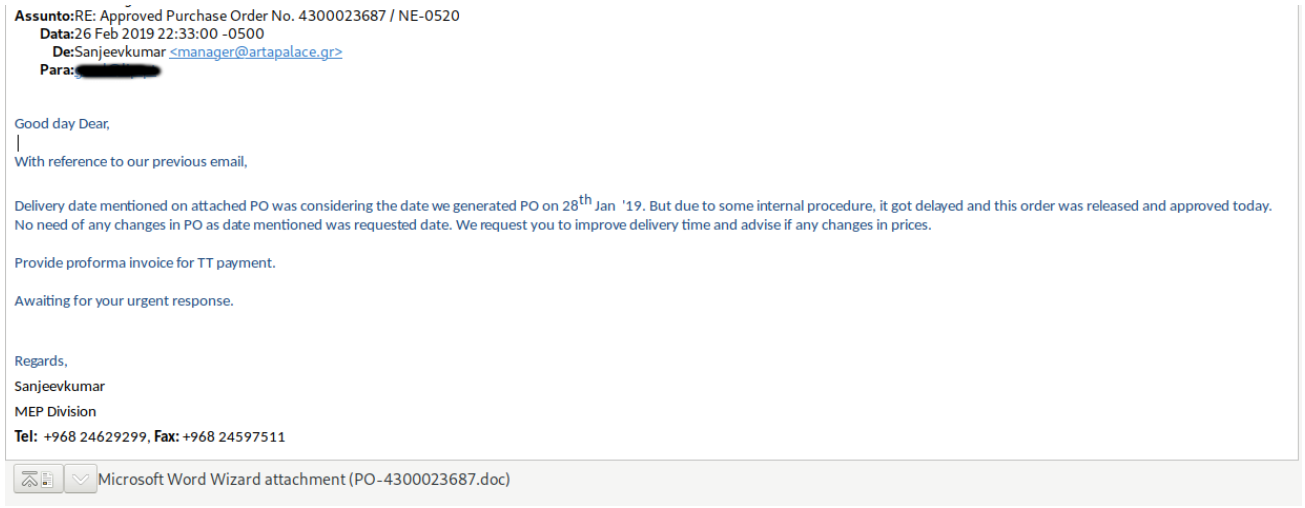
Esta mensagem eletrônica é confidencial. Sua utilização, cópia, distribuição ou divulgação são expressamente proibidas, sob pena de responsabilização civil e criminal.

E-mail nº 20184667946475529.

Electronic Mail

SPAM

- ✔ **Phishing**
- ✔ **Ransomware**



Assunto:RE: Approved Purchase Order No. 4300023687 / NE-0520
Data:26 Feb 2019 22:33:00 -0500
De: Sanjeevkumar <manager@artapalace.gr>
Para:[redacted]

Good day Dear,

With reference to our previous email,

Delivery date mentioned on attached PO was considering the date we generated PO on 28th Jan '19. But due to some internal procedure, it got delayed and this order was released and approved today. No need of any changes in PO as date mentioned was requested date. We request you to improve delivery time and advise if any changes in prices.

Provide proforma invoice for TT payment.

Awaiting for your urgent response.

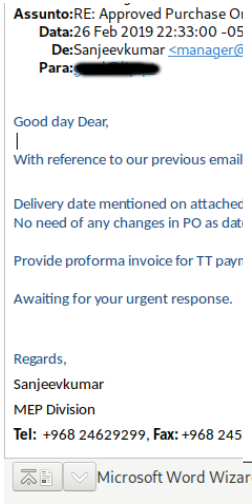
Regards,
Sanjeevkumar
MEP Division
Tel: +968 24629299, **Fax:** +968 24597511

Microsoft Word Wizard attachment (PO-4300023687.doc)

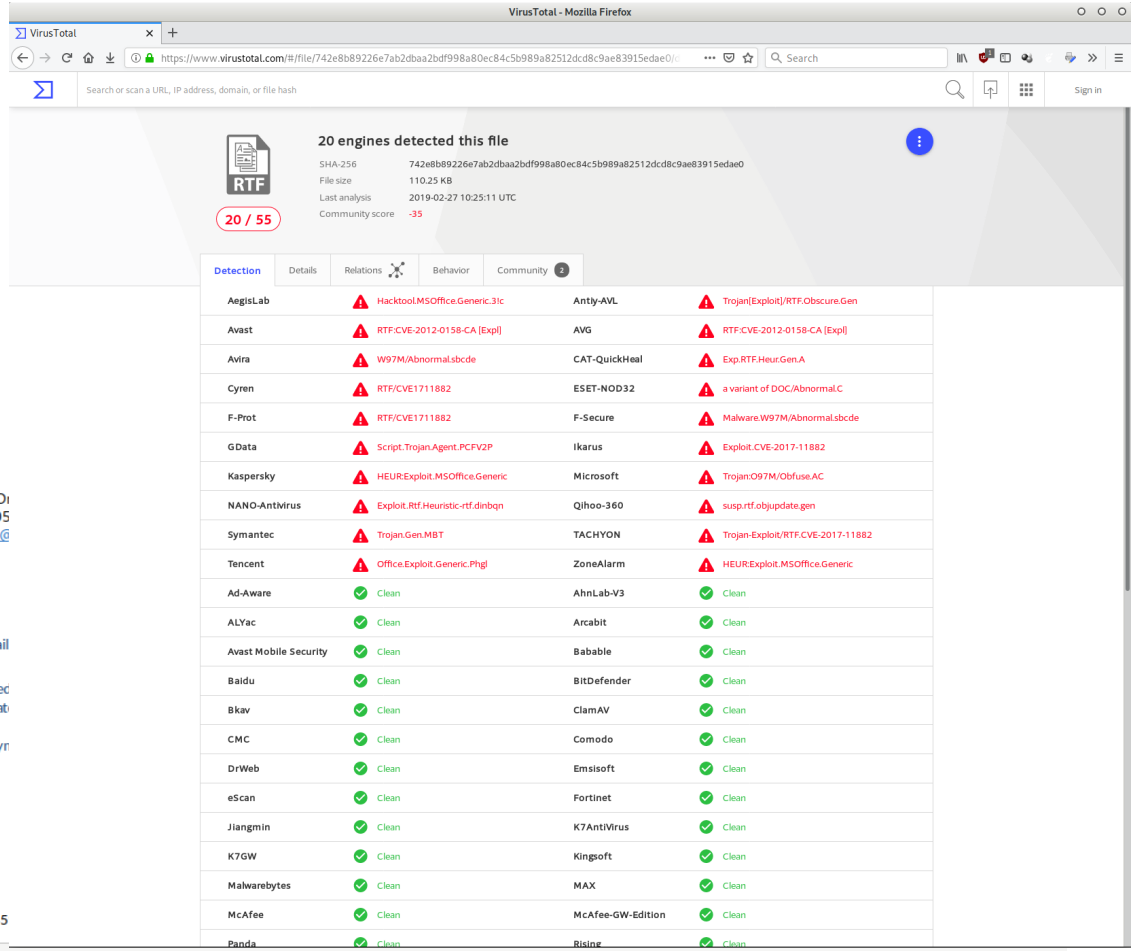
Electronic Mail

SPAM

- ✔ **Phishing**
- ✔ **Ransomware**



http://www.virustotal.com



Electronic Mail

SPAM

- ✔ **Phishing**
- ✔ **Ransomware**

From: [redacted]
To: [redacted]
Subject: Caution! Attack hackers to your account!
Date: Tue, 26 Feb 2019 13:00:22 +0100 (*26/02/19 12:00:22*)

Hi!

As you may have noticed, I sent you an email from your account.
This means that I have full access to your account.

I've been watching you for a few months now.
The fact is that you were infected with malware through an adult site that you visited.

If you are not familiar with this, I will explain.
Trojan Virus gives me full access and control over a computer or other device.
This means that I can see everything on your screen, turn on the camera and microphone, but you do not know about it.

I also have access to all your contacts and all your correspondence.

Why your antivirus did not detect malware?
Answer: My malware uses the driver, I update its signatures every 4 hours so that your antivirus is silent.

I made a video showing how you satisfy yourself in the left half of the screen, and in the right half you see the video that you watched.
With one click of the mouse, I can send this video to all your emails and contacts on social networks.
I can also post access to all your e-mail correspondence and messengers that you use.

If you want to prevent this,
transfer the amount of $768 to my bitcoin address (if you do not know how to do this, write to Google: "Buy Bitcoin").

My bitcoin address (BTC Wallet) is: 1GoWy5yMzh3XXBiYxLU9tKCBMgibpznGio

After receiving the payment, I will delete the video and you will never hear me again.
I give you 48 hours to pay.
I have a notice reading this letter, and the timer will work when you see this letter.

Filing a complaint somewhere does not make sense because this email cannot be tracked like my bitcoin address.
I do not make any mistakes.

If I find that you have shared this message with someone else, the video will be immediately distributed.

Best regards!

2. Passwords

Or other secrets

Passwords

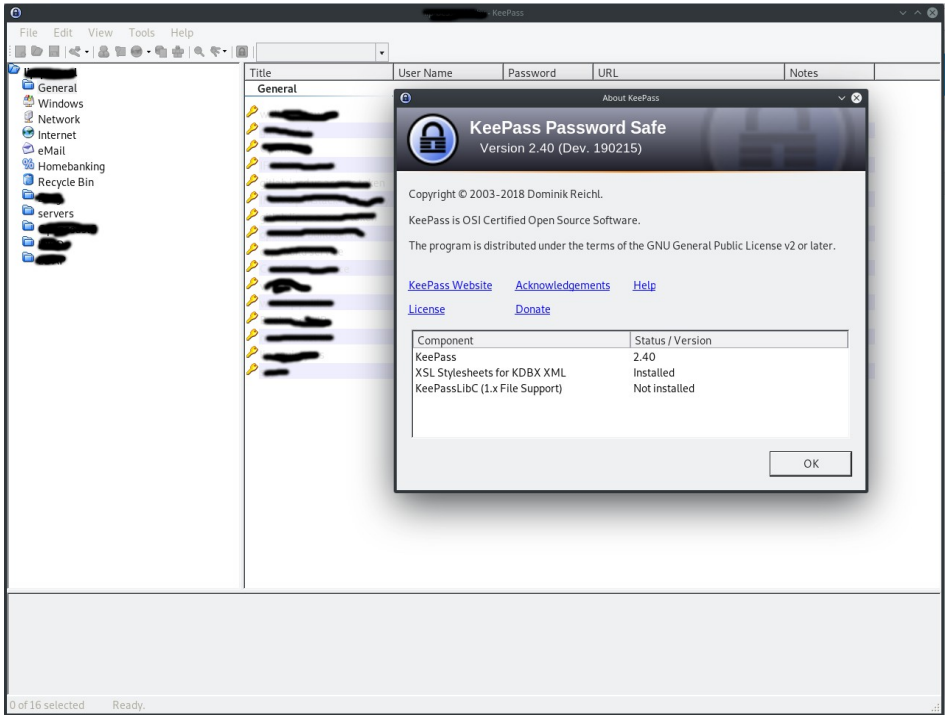
- Unique Credentials
- Password (Min. 8 Characters)
- Public Resources (Pcs, Wifi, others)
- SSH Keys
- Encryption with GPG/PGP
- Theft/Loss of equipment
- Encryption of partition with EncFS

Passwords

- Unique Credentials
- Password (Min. 8 Characters)
- Public Resources (Pcs, Wifi, others)
- SSH Keys
- Encryption with GPG/PGP
- Theft/Loss of equipment
- Encryption of partition with EncFS

Passwords

- KeePass
- Keepassx
- Keepassx0
- Keepassx2
- keepassxc



Passwords

- Unique Credentials
- Password (Min. 8 Characters)
- Public Resources (Pcs, Wifi, others)
- SSH Keys
- Encryption with GPG/PGP
- Theft/Loss of equipment
- Encryption of partition with EncFS

Passwords

- Unique Credentials
- Password (Min. 8 Characters)
- Public Resources (Pcs, Wifi, others)
- SSH Keys
- Encryption with GPG/PGP
- Theft/Loss of equipment
- Encryption of partition with EncFS

SSH Keys

[ndias@lnlip01 ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/csys/ndias/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/csys/ndias/.ssh/id_rsa.
Your public key has been saved in /home/csys/ndias/.ssh/id_rsa.pub.

[ndias@lnlip01 ~]$ scp .ssh/id_rsa.pub fermi:
[ndias@fermi ~]$ cat id_rsa.pub >> .ssh/authorized_keys
[ndias@fermi ~]$ ls -la .ssh/id_rsa
-rw------- 1 xxxxx users 1766 Jan 25 2017 .ssh/id_rsa

And protect your **HOME**
drwxrwxrwx+ 214 xxxxx users 28672 Jan 30 16:35 .
drwxr-xr-x+ 214 xxxxx users 28672 Jan 30 16:35 .

Passwords

- Unique Credentials
- Password (Min. 8 Characters)
- Public Resources (Pcs, Wifi, others)
- SSH Keys
- Encryption with GPG/PGP
- Theft/Loss of equipment
- Encryption of partition with EncFS

Passwords

- Unique Credentials
- Password (Min. 8 Characters)
- Public Resources (Pcs, Wifi, others)
- SSH Keys
- Encryption with GPG/PGP
- Theft/Loss of equipment
- Encryption of partition with EncFS

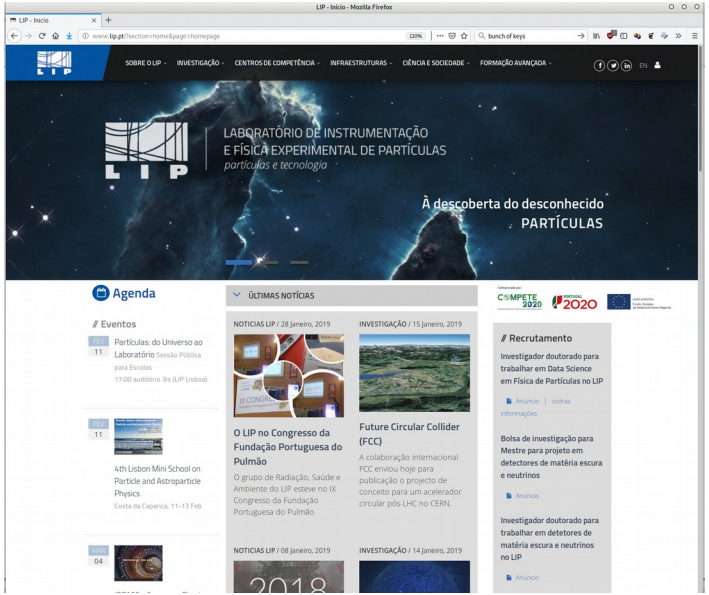
Passwords

- Unique Credentials
- Password (Min. 8 Characters)
- Public Resources (Pcs, Wifi, others)
- SSH Keys
- Encryption with GPG/PGP
- Theft/Loss of equipment
- Encryption of partition with EncFS

3.
Web Pages

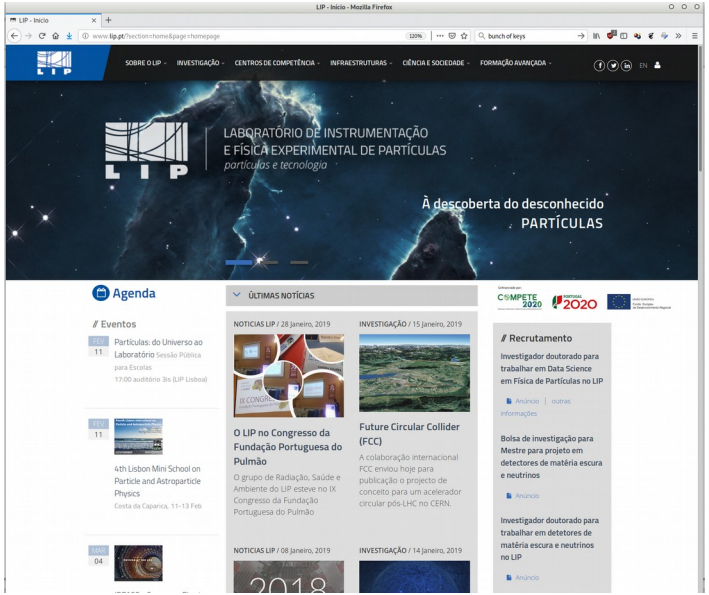
Web Pages

- Sensitive information
  Personal webpage or Social Networks
- Http ou https?
- .../index.[html|php|*] (../fotos/; ../secret/)
- API's, libs, code
- Copyright!
- Databases



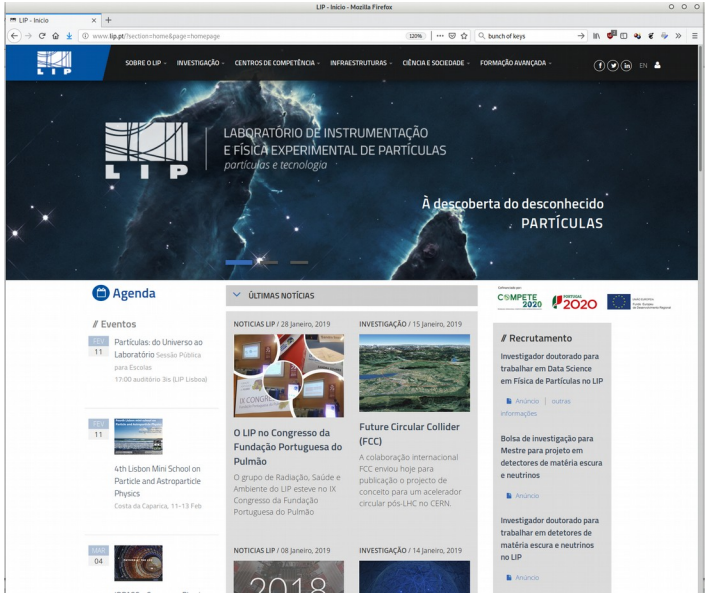
Web Pages

- Sensitive information
  Personal webpage or Social Networks
- Http ou https?
- .../index.[html|php|*] (../fotos/; ../secret/)
- API's, libs, code
- Copyright!
- Databases



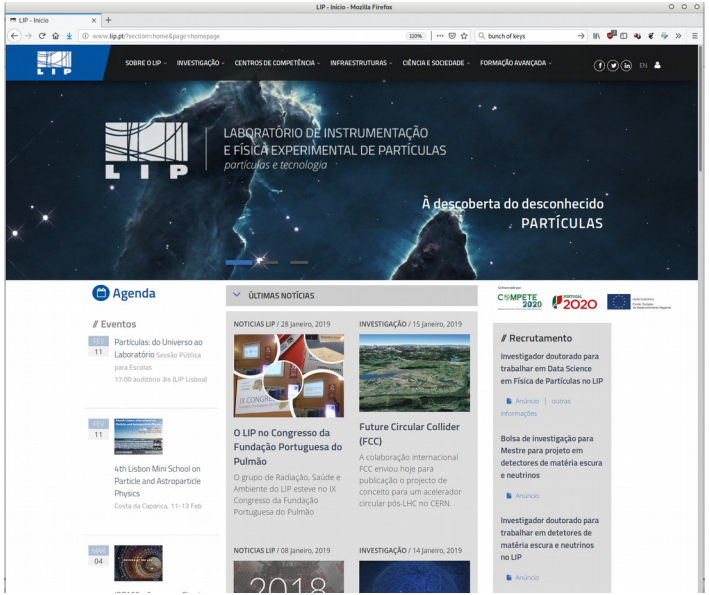
Web Pages

- Sensitive information
  Personal webpage or Social Networks
- Http ou https?
- .../index.[html|php|*] (../fotos/; ../secret/)
- API's, libs, code
- Copyright!
- Databases



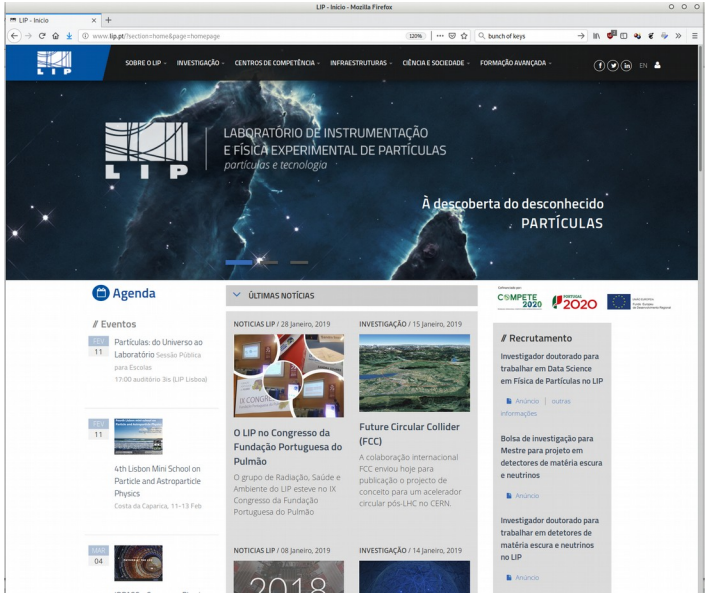
Web Pages

- Sensitive information
  Personal webpage or Social Networks
- Http ou https?
- .../index.[html|php|*] (../fotos/; ../secret/)
- API's, libs, code
- Copyright!
- Databases



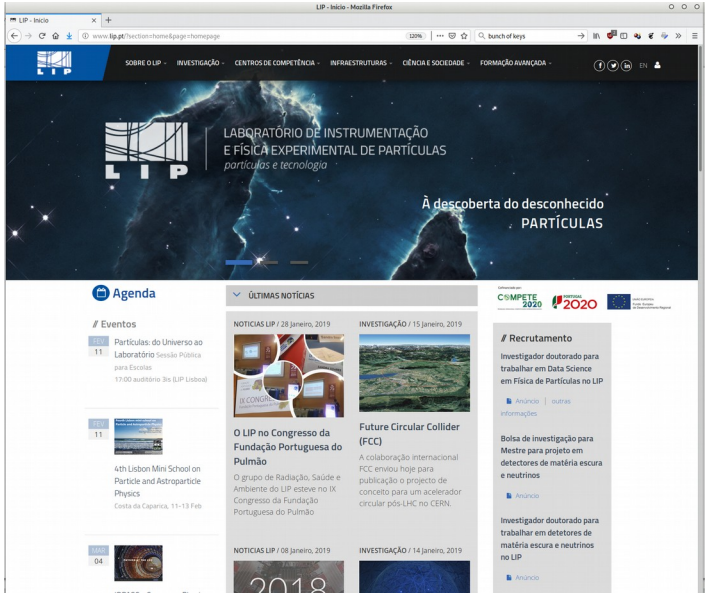
Web Pages

- Sensitive information
  Personal webpage or Social Networks
- Http ou https?
- .../index.[html|php|*] (../fotos/; ../secret/)
- API's, libs, code
- Copyright!
- Databases



Web Pages

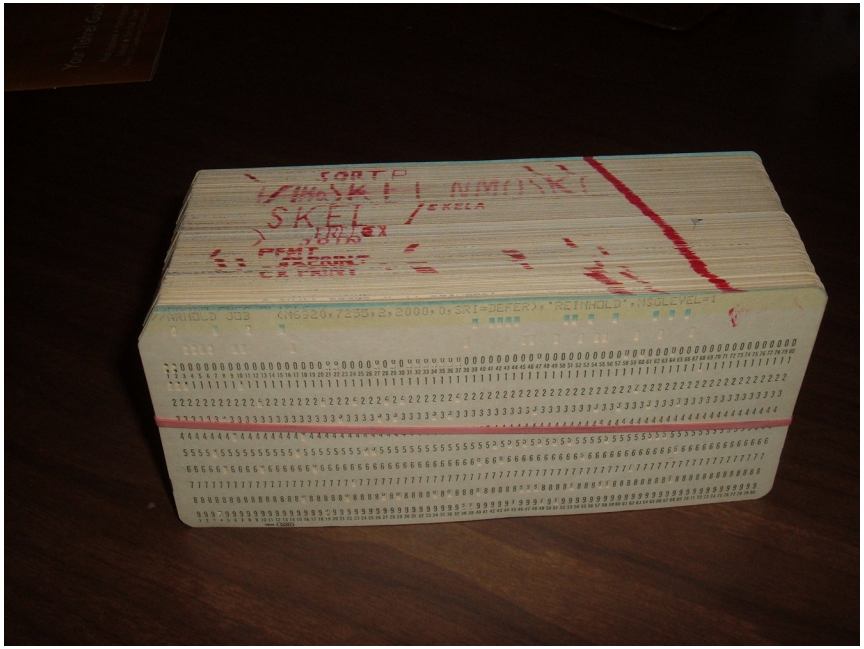
- Sensitive information
  Personal webpage or Social Networks
- Http ou https?
- .../index.[html|php|*] (../fotos/; ../secret/)
- API's, libs, code
- Copyright!
- Databases



4.
Software

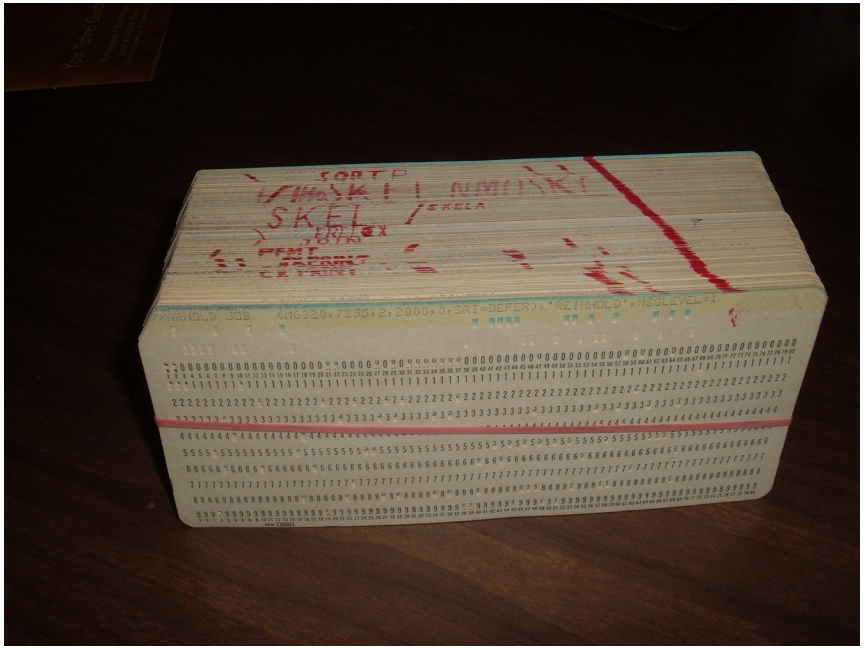
Software

- Proprietary, Licence!
- Open Source
- Updates
- Anti-Virus
- Browsers
- Mobile equipments
  Phone, Tablet, others
- P2P
- VM/Containers
- Firewall
- Services
- VPN



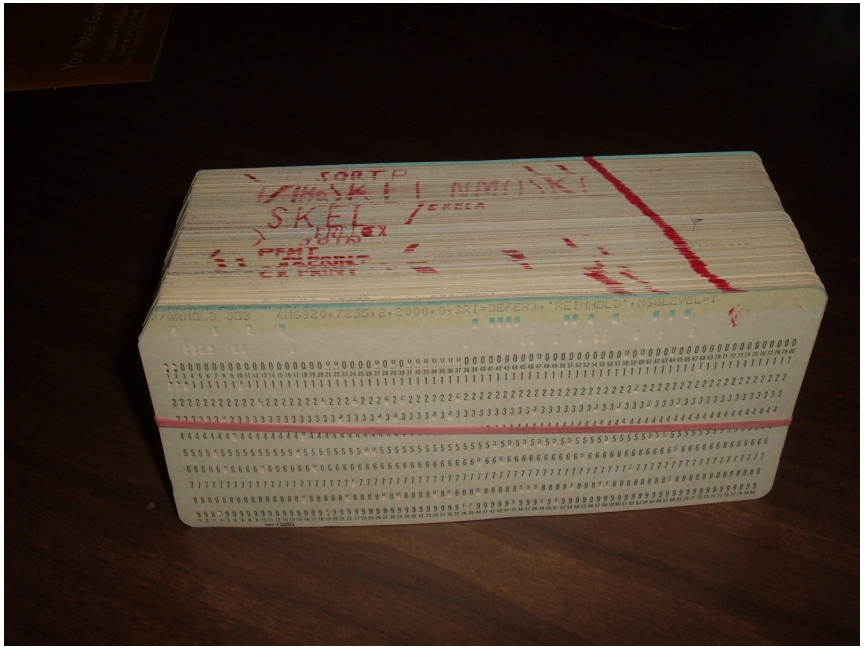
Software

- Proprietary, Licence!
- Open Source
- Updates
- Anti-Virus
- Browsers
- Mobile equipments
  Phone, Tablet, others
- P2P
- VM/Containers
- Firewall
- Services
- VPN



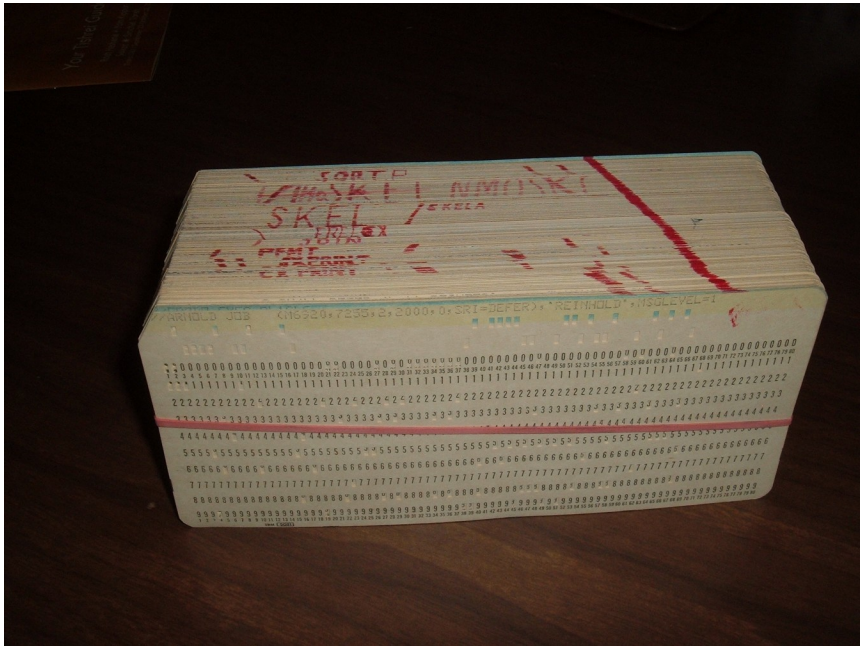
Software

- Proprietary, Licence!
- Open Source
- Updates
- Anti-Virus
- Browsers
- Mobile equipments
  Phone, Tablet, others
- P2P
- VM/Containers
- Firewall
- Services
- VPN



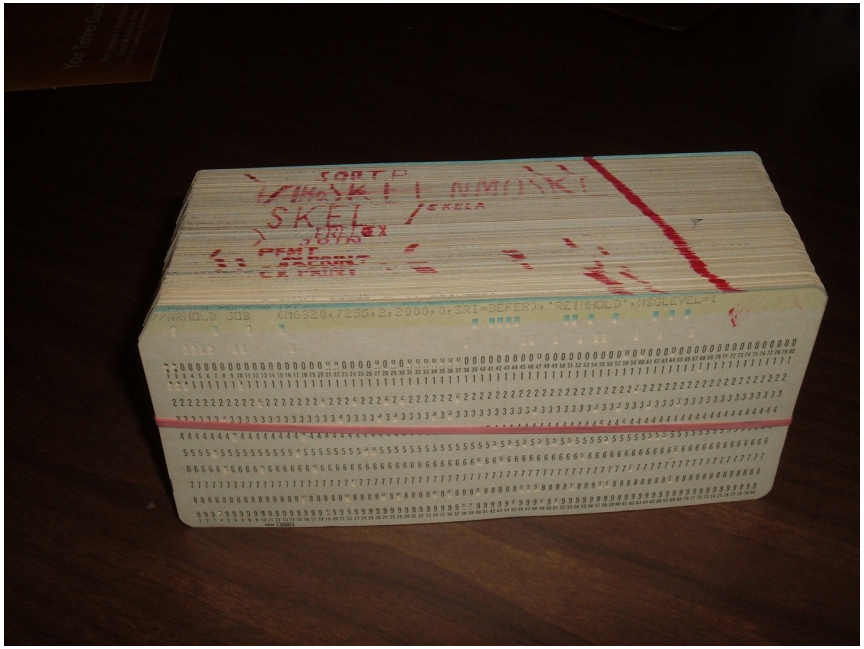
Software

- Proprietary, Licence!
- Open Source
- Updates
- Anti-Virus
- Browsers
- Mobile equipments
  Phone, Tablet, others
- P2P
- VM/Containers
- Firewall
- Services
- VPN



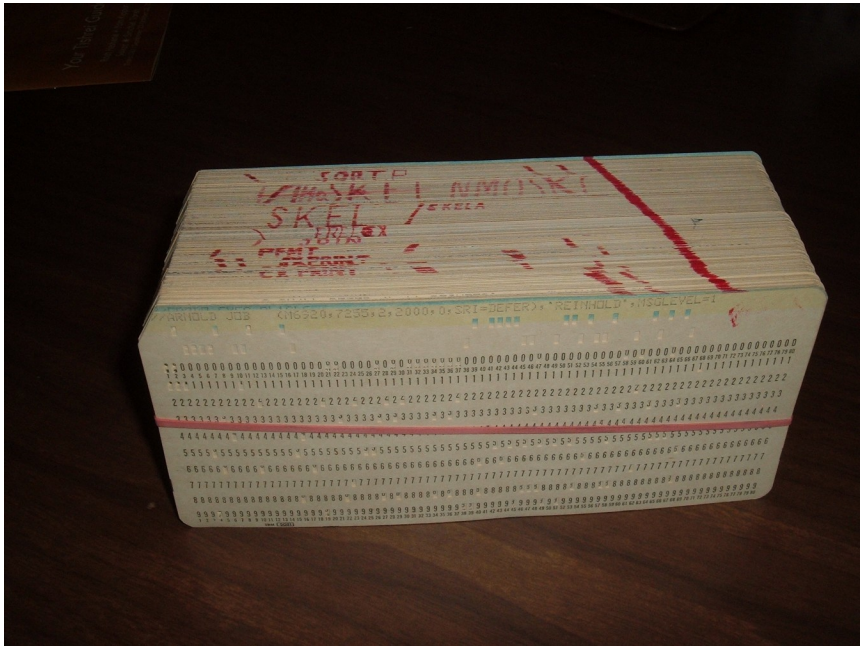
Software

- Proprietary, Licence!
- Open Source
- Updates
- Anti-Virus
- Browsers
- Mobile equipments
  Phone, Tablet, others
- P2P
- VM/Containers
- Firewall
- Services
- VPN



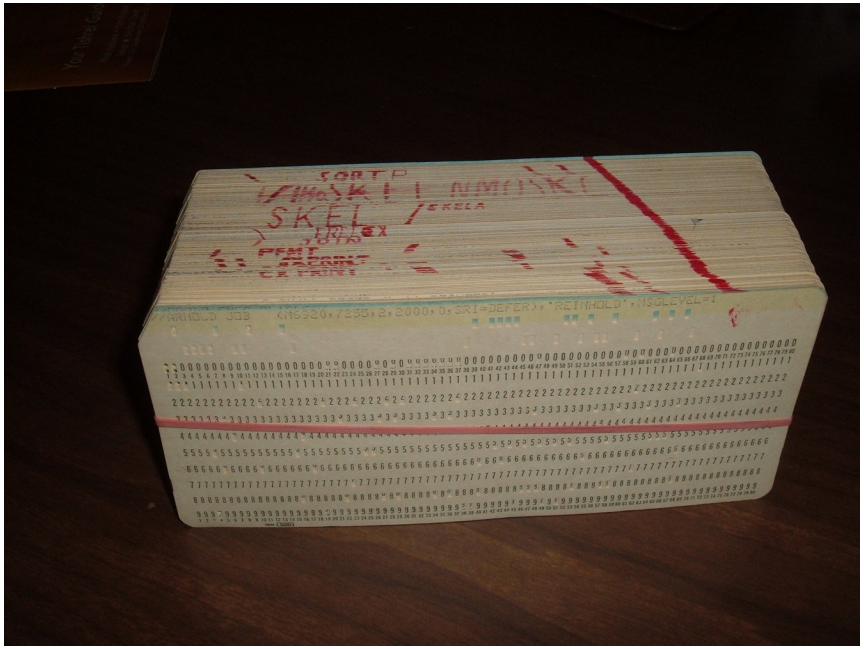
Software

- Proprietary, Licence!
- Open Source
- Updates
- Anti-Virus
- Browsers
- Mobile equipments
  Phone, Tablet, others
- P2P
- VM/Containers
- Firewall
- Services
- VPN



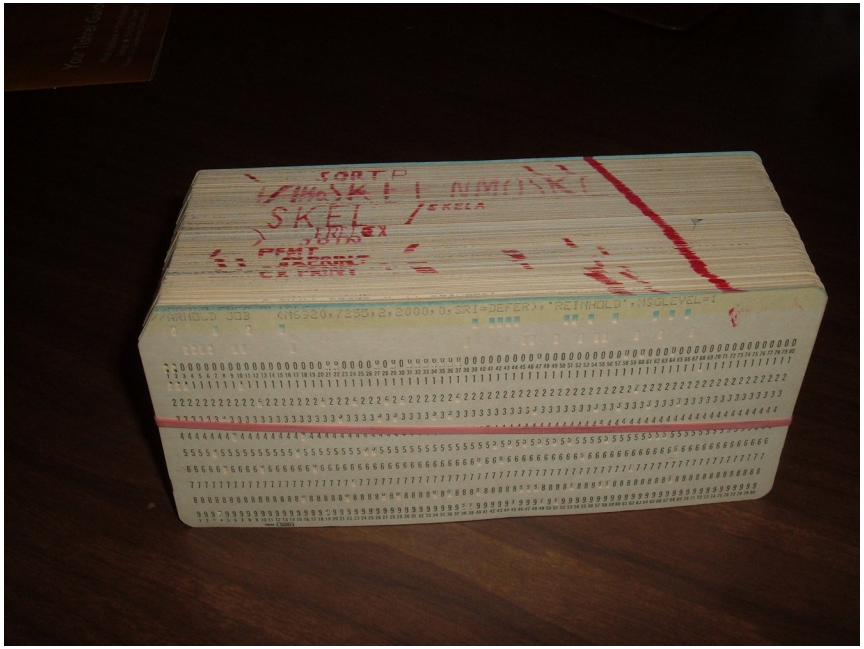
Software

- Proprietary, Licence!
- Open Source
- Updates
- Anti-Virus
- Browsers
- Mobile equipments
  Phone, Tablet, others
- P2P
- VM/Containers
- Firewall
- Services
- VPN



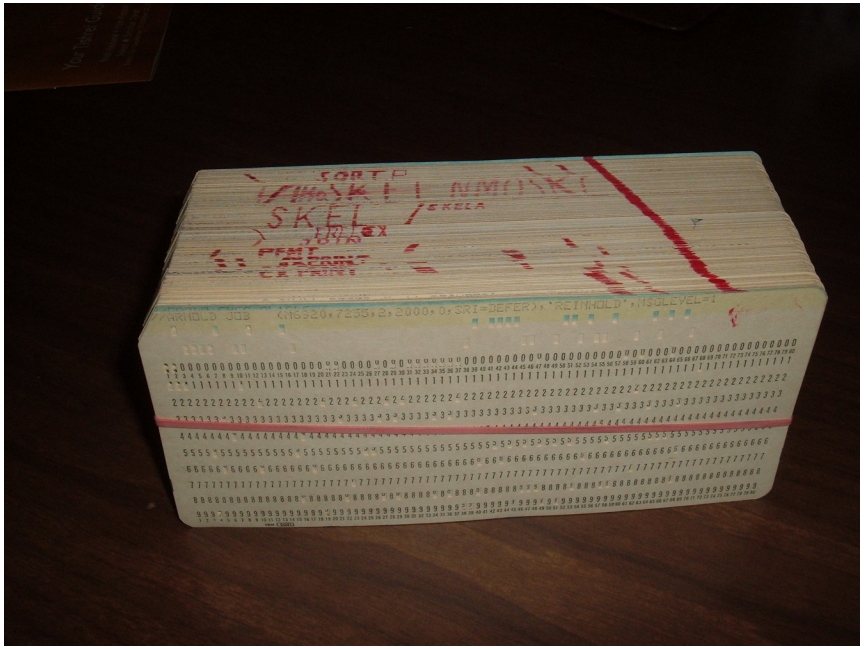
Software

- Proprietary, Licence!
- Open Source
- Updates
- Anti-Virus
- Browsers
- Mobile equipments
  Phone, Tablet, others
- P2P
- VM/Containers
- Firewall
- Services
- VPN



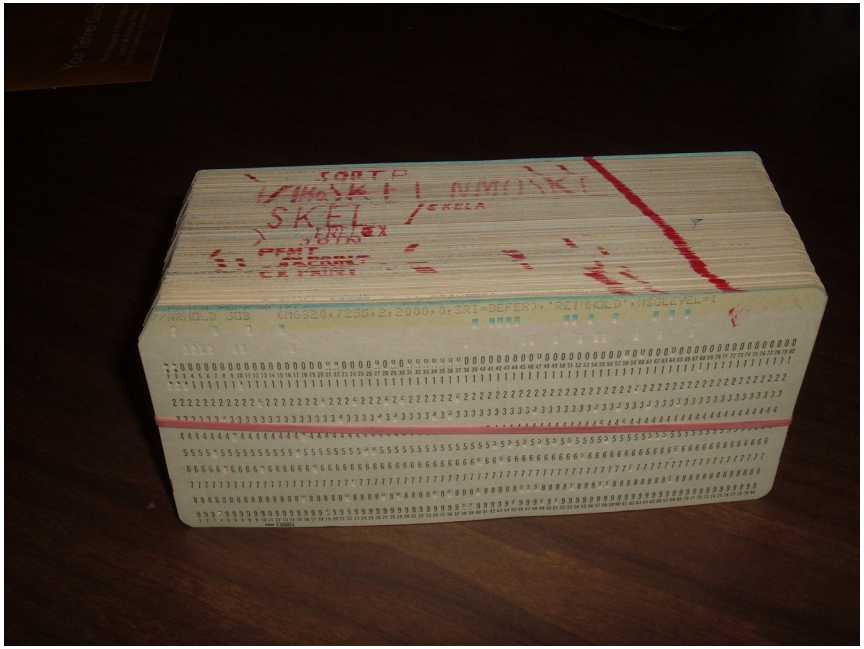
Software

- Proprietary, Licence!
- Open Source
- Updates
- Anti-Virus
- Browsers
- Mobile equipments
  Phone, Tablet, others
- P2P
- VM/Containers
- Firewall
- Services
- VPN



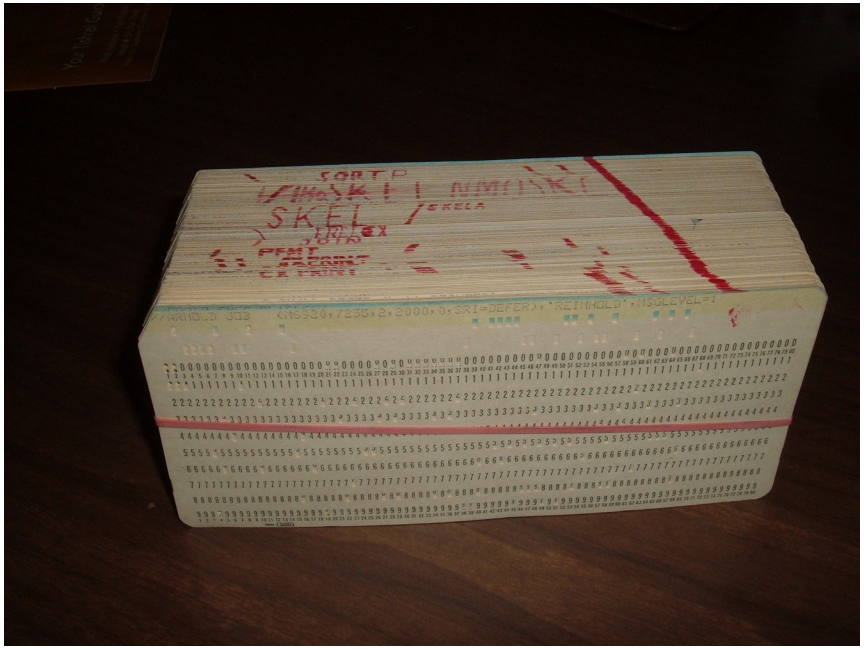
Software

- Proprietary, Licence!
- Open Source
- Updates
- Anti-Virus
- Browsers
- Mobile equipments
  Phone, Tablet, others
- P2P
- VM/Containers
- Firewall
- Services
- VPN



Software

- Proprietary, Licence!
- Open Source
- Updates
- Anti-Virus
- Browsers
- Mobile equipments
  Phone, Tablet, others
- P2P
- VM/Containers
- Firewall
- Services
- VPN



5.
Backup

Backups

- Passwords
- Computer
- Phone/Tablet
- Incremental
- Cloud/Offsite

Backups

- Passwords
- Computer
- Phone/Tablet
- Incremental
- Cloud/Offsite

Backups

- Passwords
- Computer
- Phone/Tablet
- Incremental
- Cloud/Offsite

Backups

- Passwords
- Computer
- Phone/Tablet
- Incremental
- Cloud/Offsite

Backups

- Passwords
- Computer
- Phone/Tablet
- Incremental
- Cloud/Offsite

Thanks!

Questions?

Always use helpdesk@lip.pt :)