Small law firms and full understanding and application of data protection rules: are they really irreconcilable?

Frequent misunderstandings and risk underestimations about security of clients' data

Warszawa September, Thursday 20th 2018

Avvocato Francesco Tregnaghi
Verona Bar Council - Italy

DIRECTIVE 95/46/EC preamble (old “privacy” directive)

Article 1 started with...” In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their **right to privacy** with respect to the processing of personal data.

GDPR preamble

REGULATION (EU) 2016/679

Art 1

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their **right to the protection of personal data**.

Different eras

- In 1995 the digital revolution was just starting. The digital data treatment, elaboration and net diffusion has started only for very big public institutions and companies.
- In 2016 even the smallest firm or professional uses a computer connected to internet, and carries a smartphone potentially full of data

From “privacy” to “data protection”

Just the introduction of the two ruling acts shows a different point of view of the European legislation, reflecting the evolution of the times.

- From “**privacy**” (I can’t sell or give away the data I manage) to “**data protection**”: More than that, I have to take positive action also to protect those data from all the risks they are exposed to in actual environments

Article 24 Responsibility of the controller

CHAPTER IV Controller and processor - Section 1 General obligations - Article 24
Responsibility of the controller

"1.Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and **to be able to demonstrate** that processing is performed in accordance with this Regulation…" (accountability)

Security breach notification

- According to Article 33, a law practice acting as data controller must notify personal data breaches to the supervisory authority without undue delay, and in any event not later than 72 hours after having become aware of such a breach.
- In certain high risk cases, the law practice is also required to notify its clients directly (Article 34), though there are special exemptions.

A general view on data protection

Protecting data you manage, apart not willingly giving them away, include:

1) Make sure data is not stolen (security, security and even more security)

2) Make sure data is not accidentally lost (redundant backup, with increased concern about security)

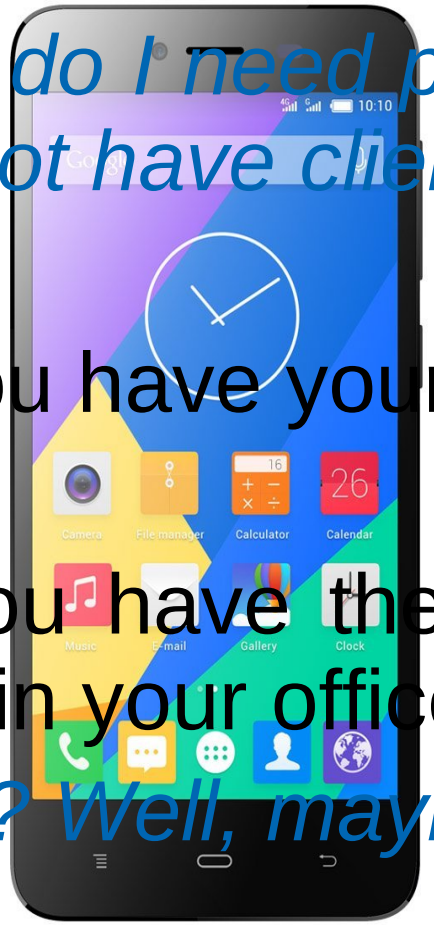
Small law firms and data protection

Every single-lawyer firm (remember: no mandatory DPO!) must understand what data protection may be

But, most of all

What is not!

1 - Unprotected Smartphones



What do I need protected access or data encryption for? I do not have clients' data on it!

Really?

Do you have your work emails on it?

Yes!

Do you have the same cloud storage access than you have in your office computer?

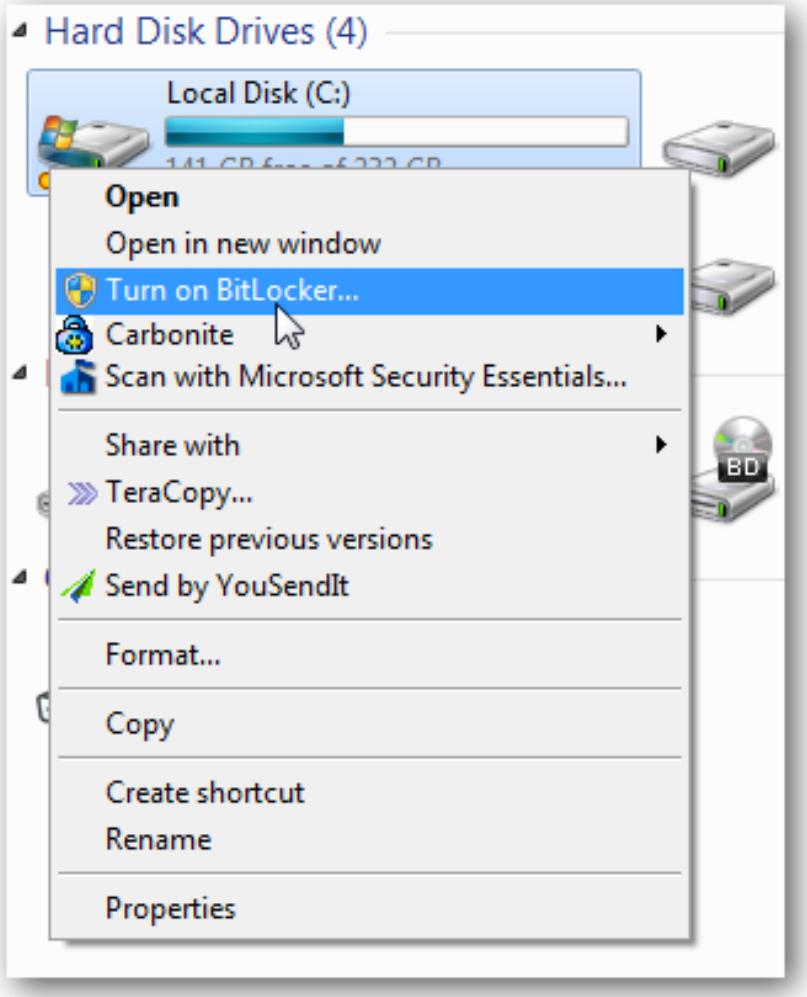
What? Well, maybe. I don't have a clue.


Verbatim

2 - Unencrypted portable backup devices

Hey, my work files and data are backupped! And, for redundancy and security, I bring them home, too!

Many Colleagues do this (and for a good reason) but if the portable device is not encrypted, this a HUGE risk for data protection!
Very few knows that is very easy to protect those devices.

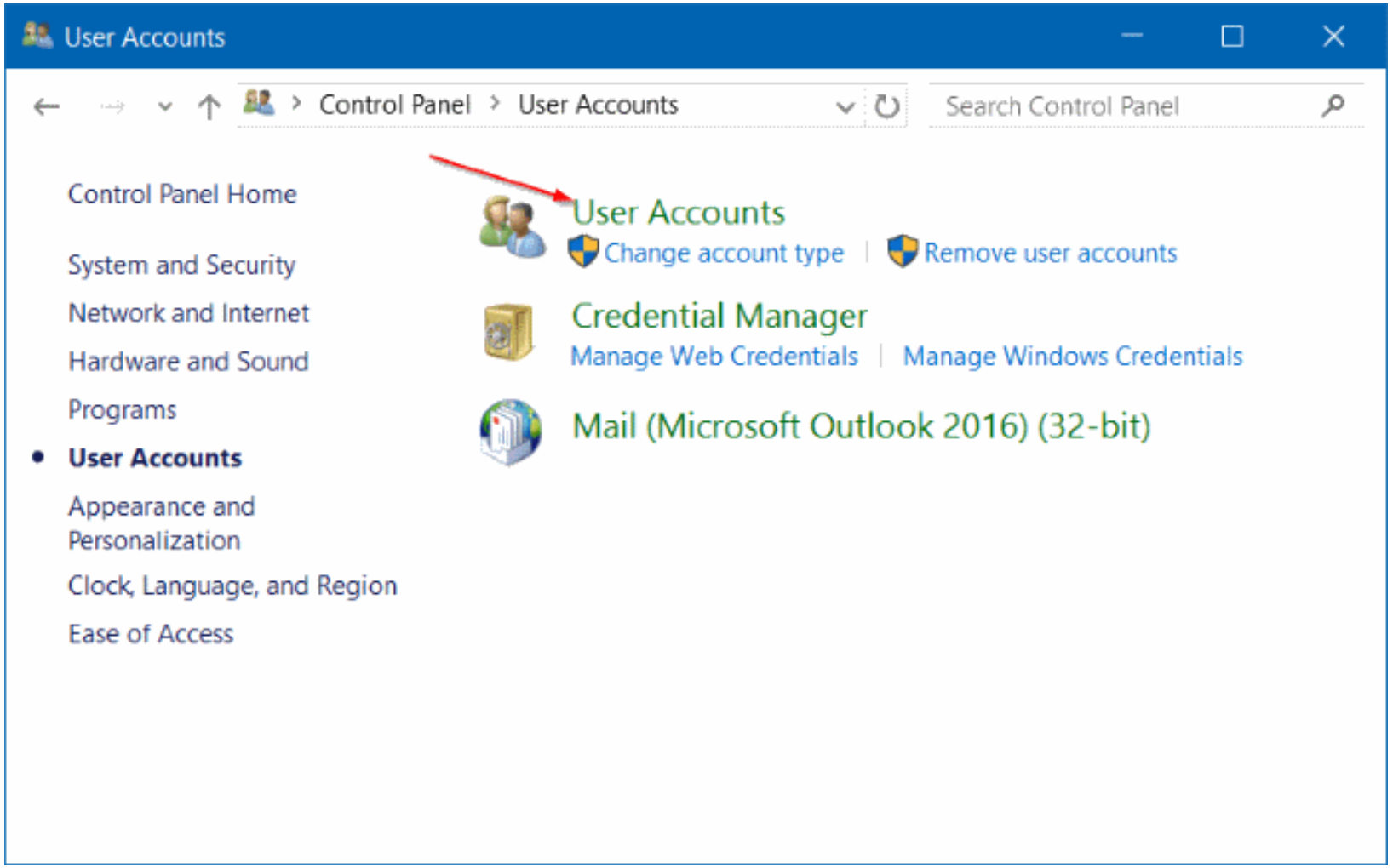


Unlocked personal computers

A frequent mistake is not to **protect the user account with a password**, or not setting the **screensaver** to ask it again whenever the screen resumes after a pause.

This helps not only unauthorized access from people in front of the physical device, but, most of all, makes **accessing the computer from the network** much, much easier.

Managing accounts is easy

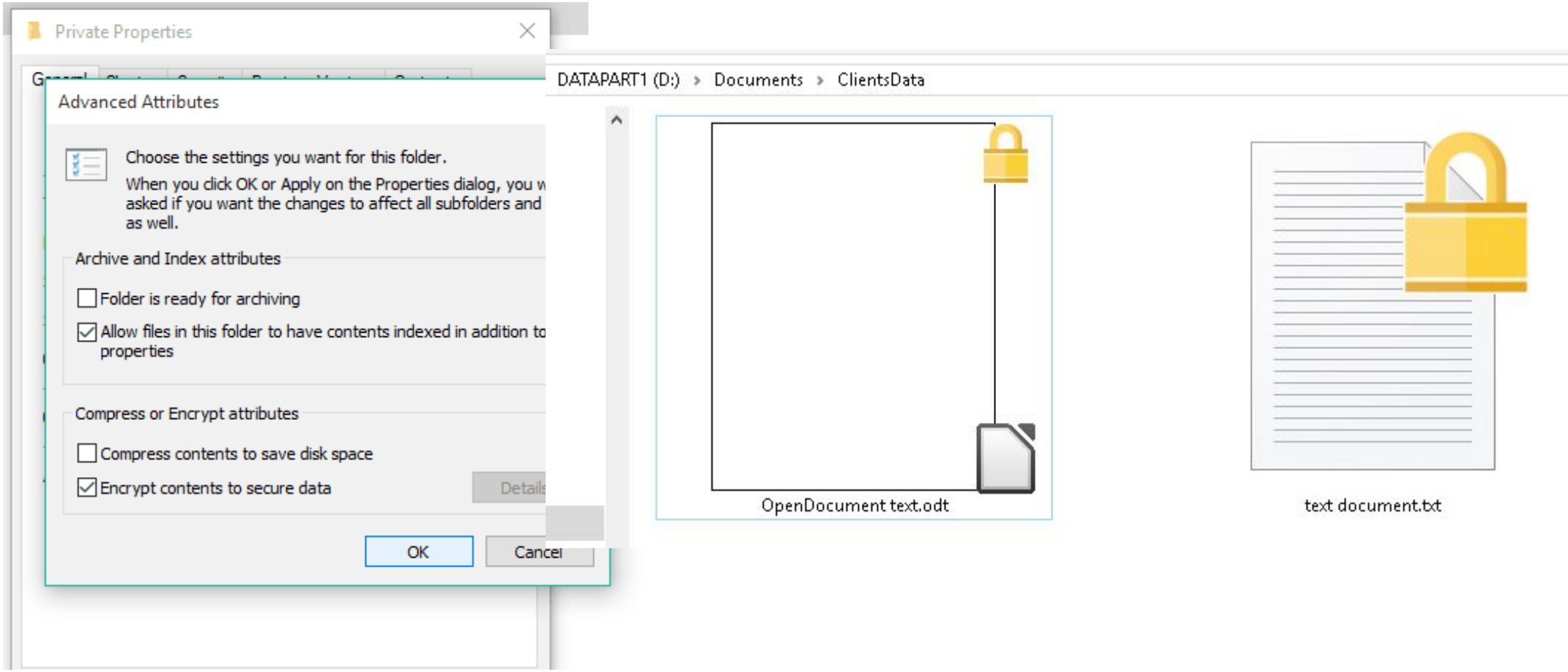


Unencrypted sensitive data

Protecting the user access means nothing is someone has in his hands the physical disk (e.g. on a stolen laptop). Accessing it from another O.S. is very easy, and all data are readable.

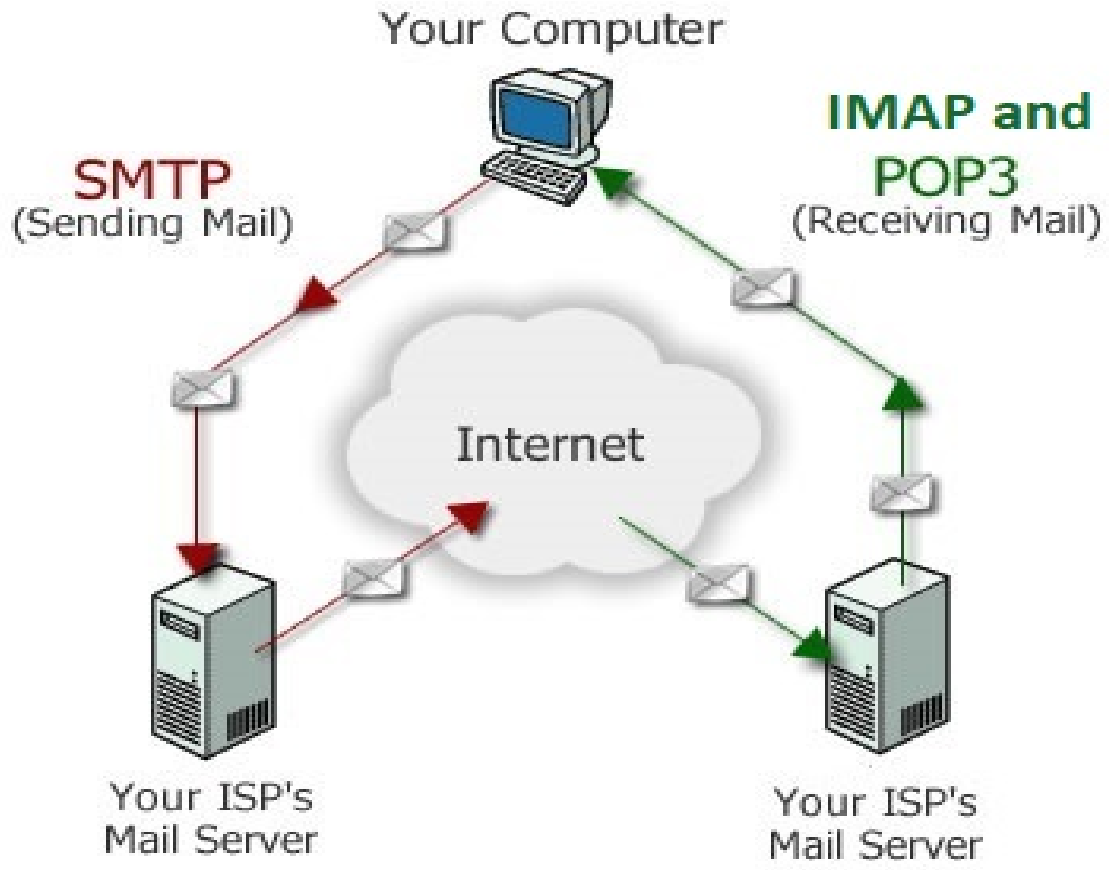
Most modern operating systems (in Windows since XP, in the highly recommendable “pro” version) have **built-in full disk encryption,** which will encrypt the entire contents of the drive. The data is decrypted when the user accesses the device. Unfortunately, it may not be enabled by default, requiring action to be activated

Activating encryption on single folders



Avv. Francesco Tregnaghi - Verona

E-Mail servers unsecure access



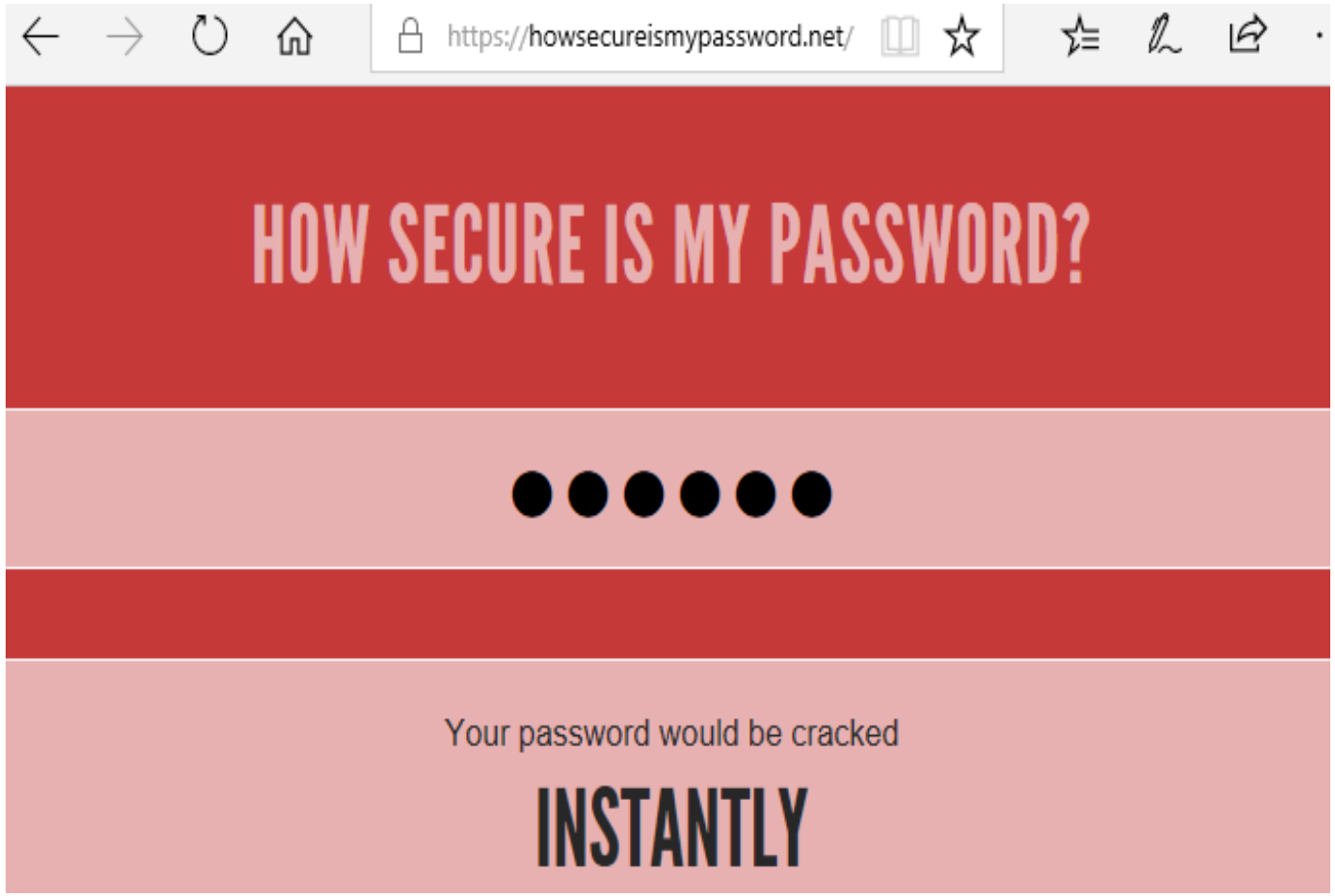
POP3, SMTP, IMAP are UNSECURE protocols.
Any good hacker, from anywhere, could read the emails in the same moment we download or upload our messages from/to mail servers. And read the passwords for future accesses, too.

The equivalent but encrypted **POP3s, SMTPs, IMAPs** (where “s” stands for secure) must be used instead.
They use one of the secure encrypted protocols

Too simple passwords

Most commonly used Pws according to Password manager “Keeper”
Rank 2016

1 123456
2 123456789
3 qwerty
4 12345678
5 111111
6 1234567890
7 1234567
8 password
9 123123
10 987654321



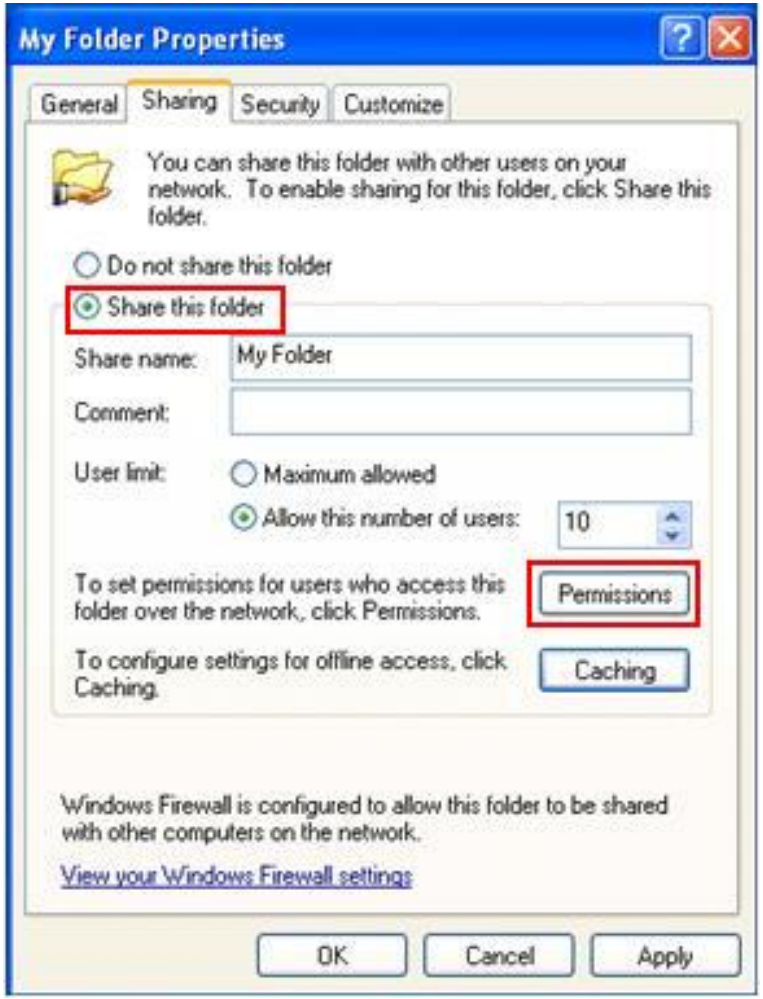
Shared LAN resources

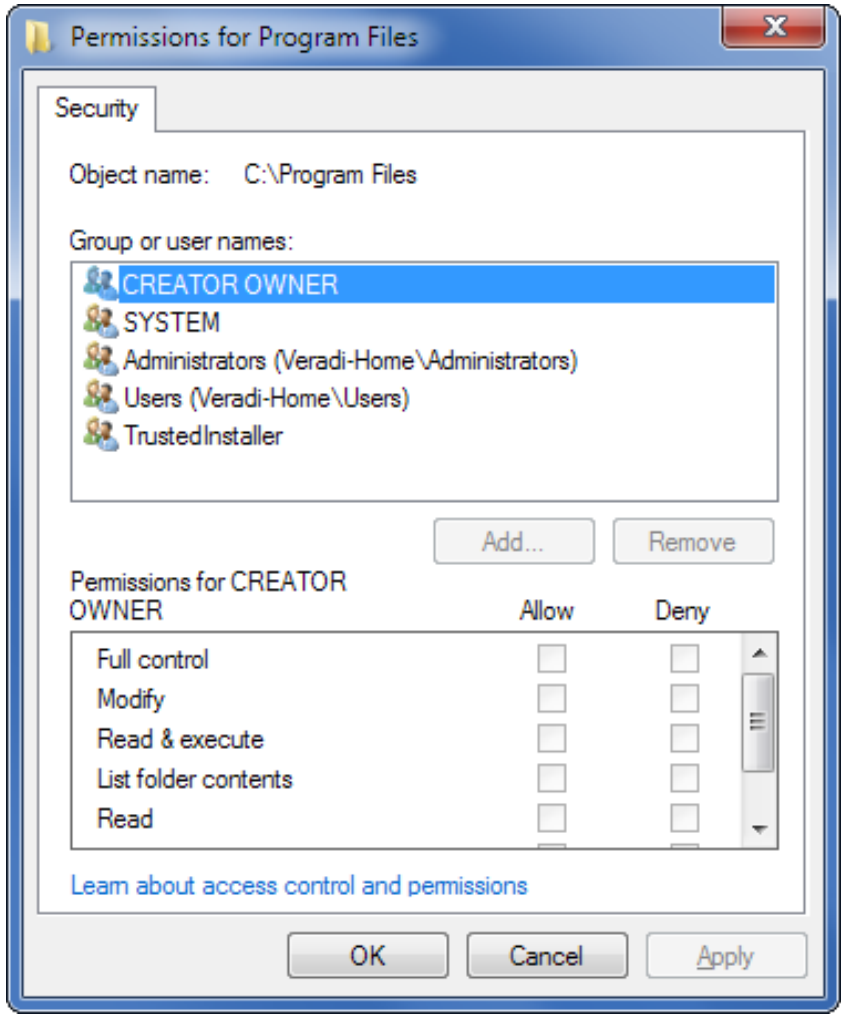
Many small law firms share the offices with colleagues or other professionals, sharing printers, internet access and LAN resources.

If the resources sharing isn't controlled and set with the needed security permissions, a lot of data may result accessible to people that should not read/copy/ modify them.

Any shared resource should be protected with correct permission policies

Managing folder permissions



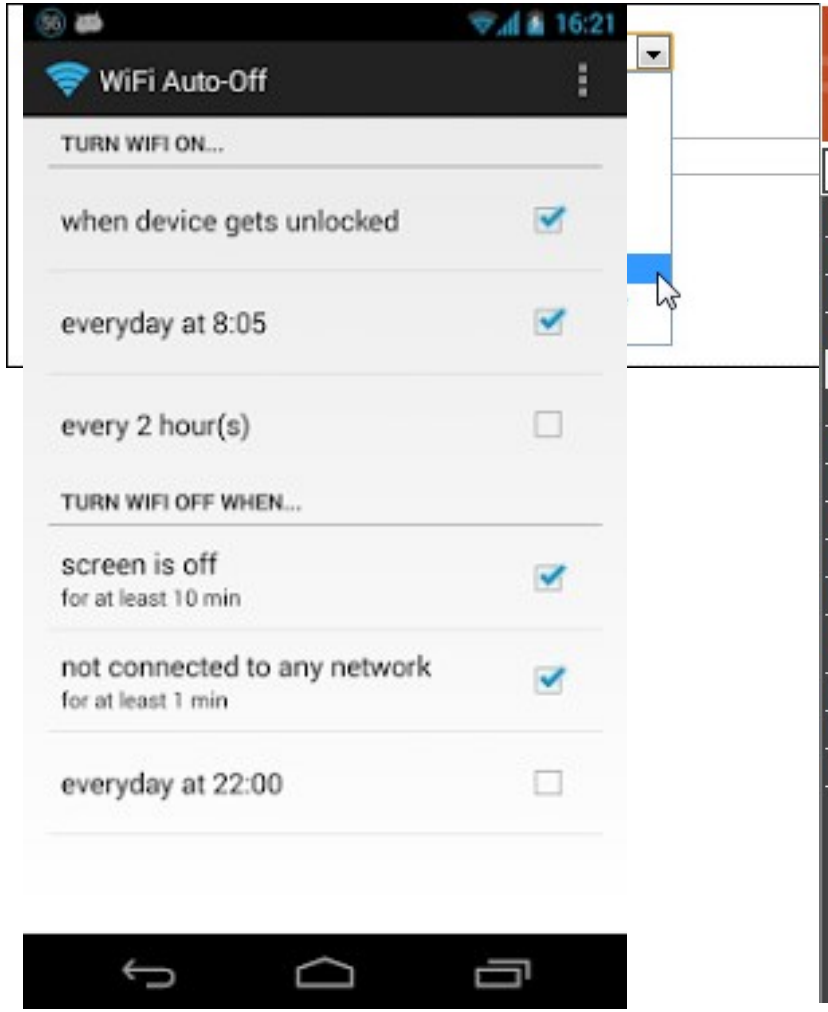


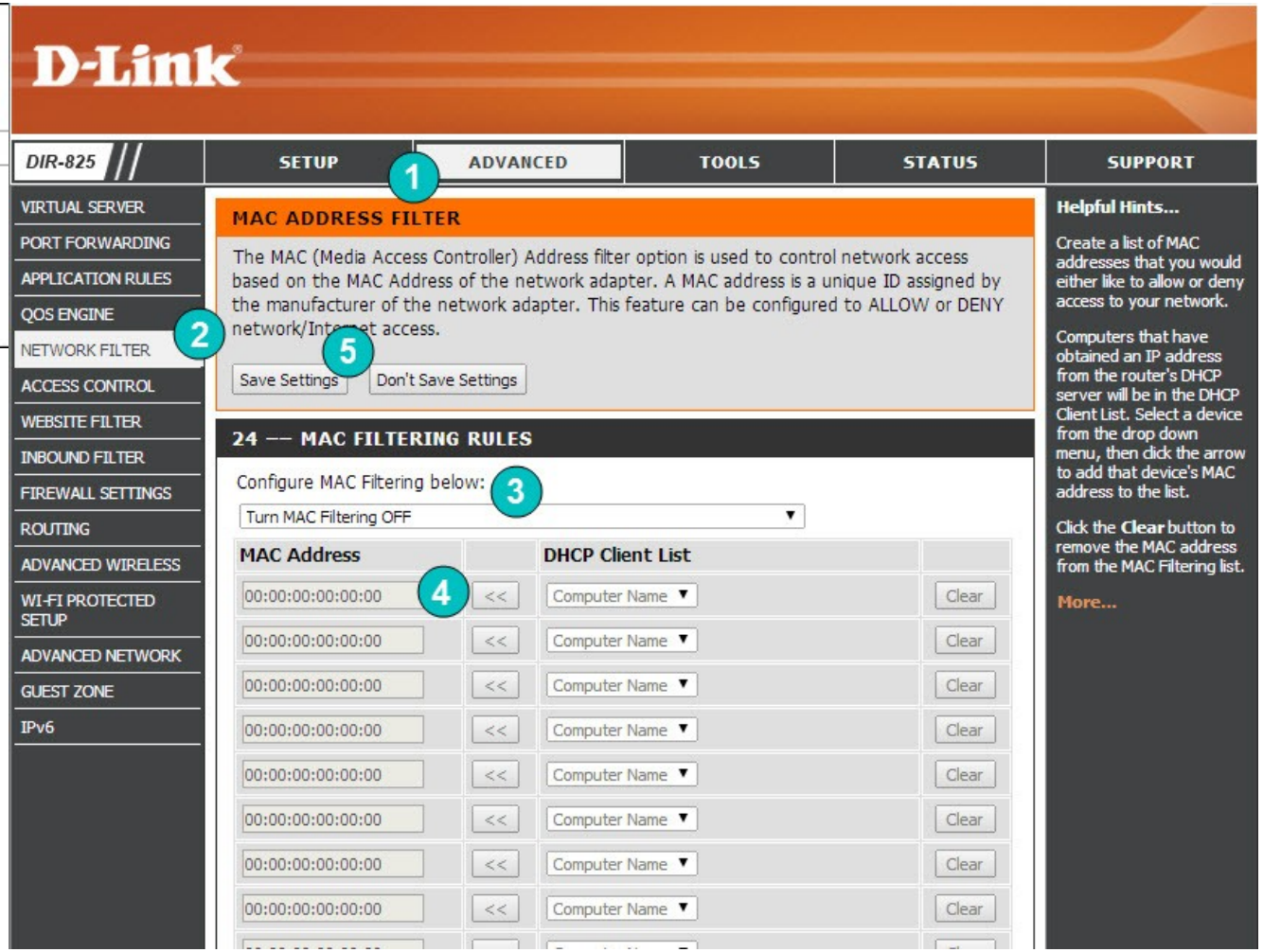
Wifi network access

WiFi access to LANs containing data should be, if necessary

- Protected by the most efficient transmission protocol
- Access should be limited to specified devices (using their MAC addresses)
- Turned off when not necessary (many WiFi routers have automatic timed turn-off and on)

WiFi settings





Multi-function printers/scanners

Modern network scanners have built-in hard-disks to store scanned documents, that will be later picked by the interested lawyer. Those files are not erased automatically. This is unacceptable in shared LANs. But, whorst...

In a recent case, a firm that bought a second-hand machine from a leasing company found a full hard-disk of PDF documents, clearly and easily identified as documents scanned by a Milan medium-sized law firm!

Cloud Storage

Cloud storage is fantastic. We can work from everywhere and the backup is assured by well organized third-parties. There are even excellent ones for free.

- It must be of course protected with a strong password.
- It should be hosted in EU since the US Patriot Act still clashes with EU data protection environment, and to store data in a server subject to it would be a violation of the EU regulations

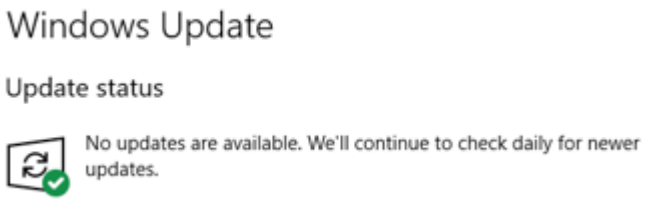
Troyan / Virus threats

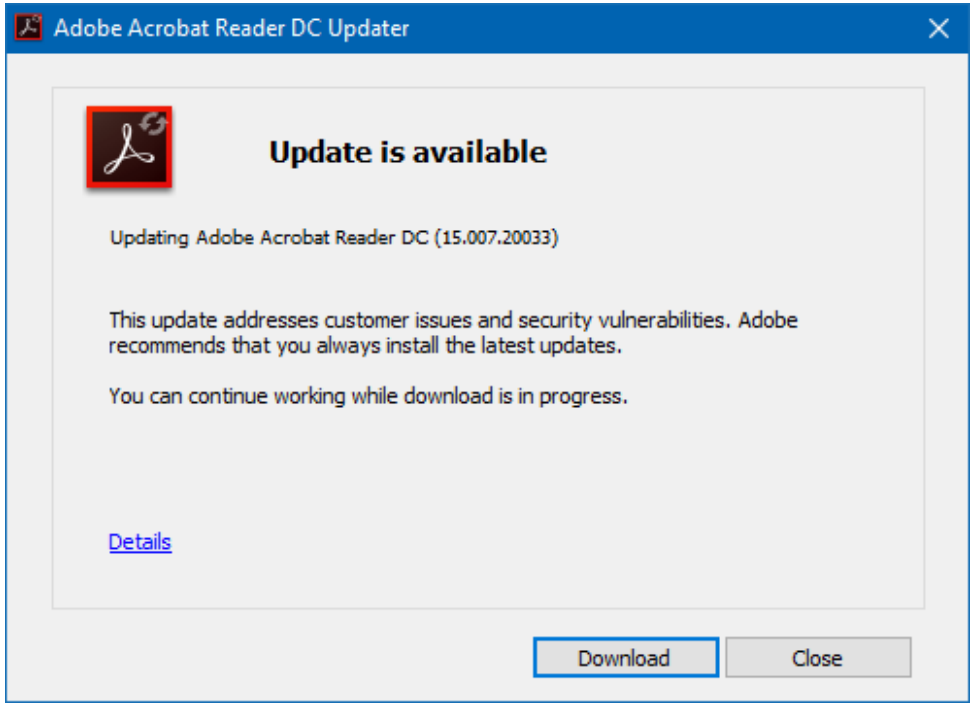
Malware may attempt both privacy and security of “our” data.

- Some are designed to secretly steal data and passwords.
- Some others (ransomware) do not steal your data, but encrypt all of them (and all the real time backups are affected, of course), and promise the decryption key only by paying a ransom. Even if you pay, sometimes all data are lost forever
- An up-to-date anti-malware/antivirus is vital, as well as backup policies that consider the risk of all the connected resources to be compromised at once.

Software updates

- All the software we use, starting from the device OS and with special regards with software with internet access, should be upgraded to the last release, to avoid security leaks.





What to do

- We need not to sleep over our habits, but consider threats are always changing, as the environment we are connected to improves.
- We have to analyze our “digital environment” to understand the risks
- We have then to plan accordingly, to erase or reduce those risks
- ...and to comply GDPR!

How can I understand the real risk in my environment?

DPIA (Data protection impact assessment, art 35) even when non-mandatory may be a very useful instrument to identify risks.

The French authority (www.cnil.fr) developed an open-source and multi-language software that may be a very useful guided instrument to analyze our data environment and identify risks

Should a lawyer become an IT expert?

- No, of course. But a certain degree of IT skill is required. If lacking, a civil or even deontological responsibility may occur (CCBE Guidance 2016)
- Even though most of the actions to take to avoid the exposed risks are not so difficult, a lawyer may use help from a technician BUT
- he personally must know the risks and make sure all of them are considered and minimized, AND
- must learn and follow the good practices in data protection in every-day's life

Francesco Tregnaghi

Avvocato – Verona, Italy

www.tregnaghi.it

 @Effetiverona

Credits:

Thanks to Francesco Paolo Micozzi, of the Cagliari Bar