Forum Lemniaci
Legnago 26 Ottobre 2018

Piccoli studi legali e GDPR: convivenza davvero impossibile?

Le frequenti “bucce di banana” nella protezione dati all’interno dello studio legale

Legnago

Avvocato Francesco Tregnaghi
Ordine avvocati di Verona

Preambolo DIRETTIVA 95/46/EC (la vecchia direttiva “privacy”)

L’art. 1 iniziava con…” Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del **diritto alla vita privata**, con riguardo al trattamento dei dati personali.

” 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.

Prembolo del GDPR

REGOLAMENTO (EU) 2016/679

Art 1 1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare **il diritto alla protezione dei dati personali**.

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**.

“Ere” differenti

- Nel 1995 la rivoluzione digitale era agli inizi. Il trattamento digitale dei dati, la loro elaborazione e la distribuzione via rete era realtà solo per istituzioni molto grandi
- In 2016 anche l’impresa minima ed il professionista che lavora da soloe da casa hanno un computer, elaborano dati dei clienti e sono connessi ad internet

Dalla “privacy” alla “protezione dei dati”

La semplice lettura dell’introduzione delle due norme rende evidente un punto di vista differente nelle due norme europee, che riflette l’evoluzione dei tempi

- Dalla “**privacy**” (Non posso vendere o cedere i dati che tratto) a “**protezione dei dati**”. Oltre che non cederli, devo prendere misure positive per proteggere quei dati anche dal rischio a cui sono sottoposti per l’esposizione nell’attuale ambiente altamente digitalizzato

Art 24 Responsabilità del titolare del trattamento

Capo IV Titolare del trattamento e responsabile del trattamento Sezione 1 Obblighi Generali - Art 24 Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario" (accountability: rendicontabilità di quanto fatto)

Notifica di una violazione dei dati personali (security breach)

- Per l’art 33 anche uno studio legale in caso di violazione dei dati personali, il titolare del trattamento deve notificare la violazione all'autorità di controllo competente senza indugio e comunque non oltre 72 ore dal momento in cui ne è venuto a conoscenza
- In determinati casi di elevato rischio per i diritti e le libertà delle persone fisiche, il titolare del trattamento (Avv.) comunica la violazione all'interessato senza ingiustificato ritardo (Art, 34), anche se ci sono speciali eccezioni.

Protezione dei dati, in generale

Proteggere i dati che si trattano, oltre non cederli volontariamente, include:

1) Assicurarsi che i dati non siano rubati (sicurezza, sicurezza ed ancora sicurezza)

2) Assicurarsi che i dati non siano accidentalmente perduti (backup ridondanti, con però incremento della preoccupazione sulla sicurezza)

Ogni singolo avvocato (ricordate? Non deve avere il DPO!) deve capire che cosa è "proteggere i dati"

Ma, soprattutto

Cosa non lo è!

Smartphone senza protezione

MA cosa mi serve a fare l'accesso protetto o la criptazione del mio telefono? Mica ci tengo dati dei clienti?!

Davvero?

Hai per caso le email di lavoro sul cellulare?

Sì!

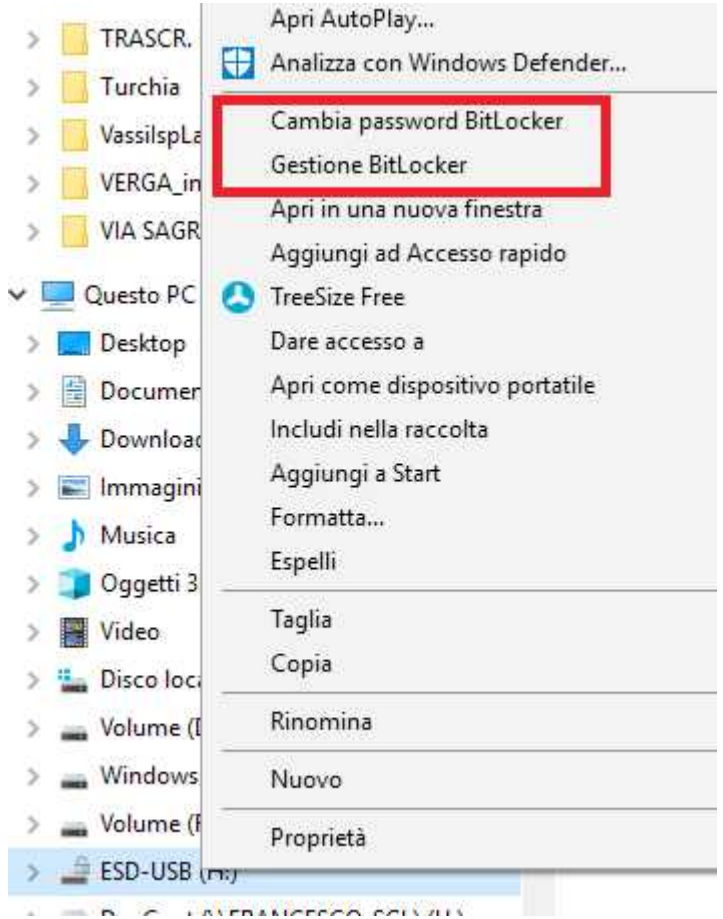
Hai per caso lo stesso servizio archiviazione cloud che usi sul tuo computer?

Che??? Boh, forse. Non ne ho idea!

Dispositivi portatili di backup non criptati

Guarda, i mie file di lavoro sono tutti backuppati! E, per sicurezza e ridondanza, me li porto anche a casa.

Molti Colleghi lo fanno (e per buone ragioni) ma se il dispositivo non è criptato c'è un ENORME rischio per la protezione dei dati!
E molto pochi sanno quanto sia facile, invece, criptare il dispositivo.

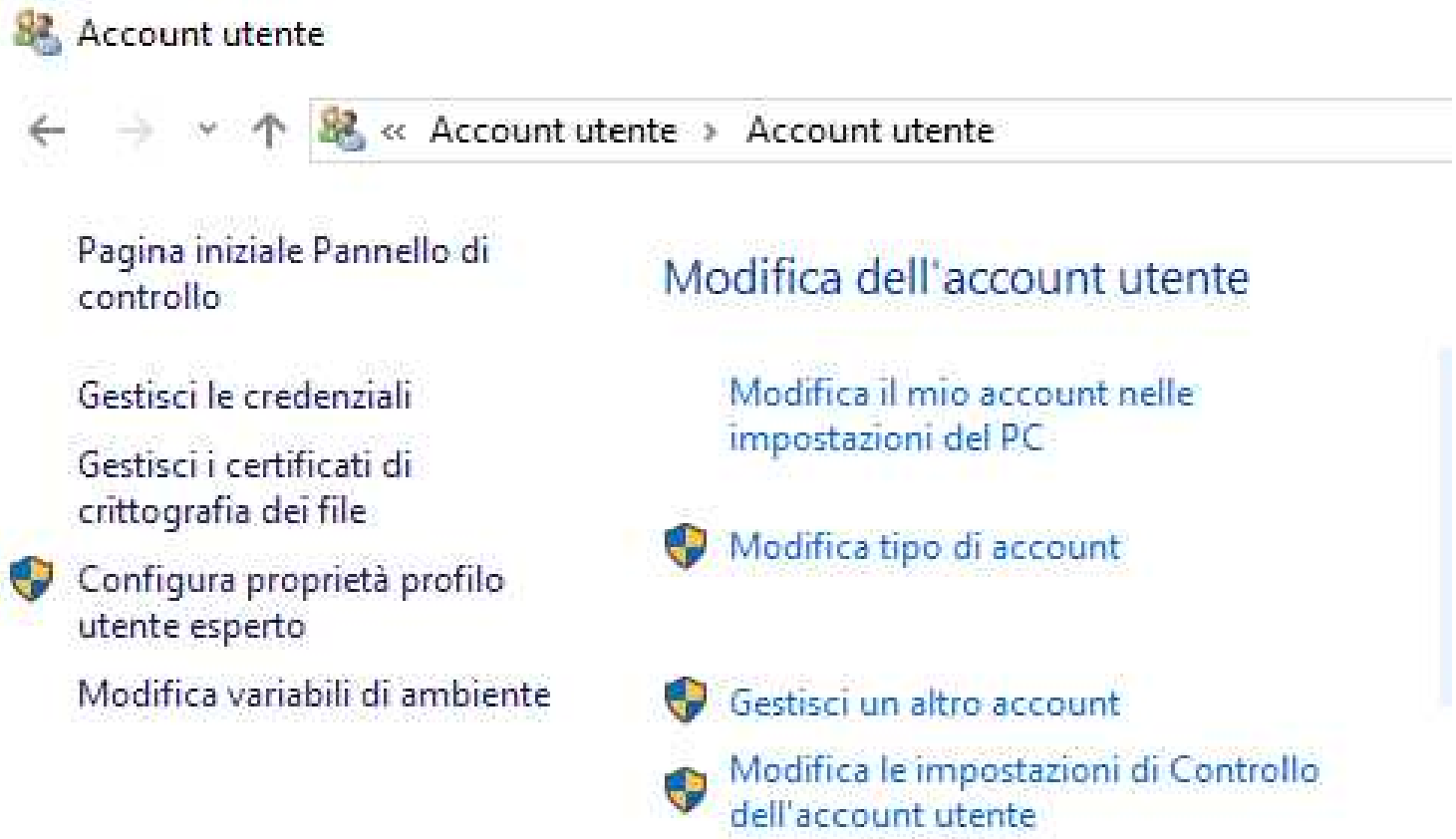


Personal computers non bloccati

Un errore frequente è non **proteggere l'account utente con una password**, o non settare lo **screensaver** in modo da richiederla ogni volta dopo la pausa.

Questo permette a persone non autorizzate ad accedervi fisicamente, ma, soprattutto, rende **accedere al computer da remoto** assai più facile

Gestire gli account utente non è difficile

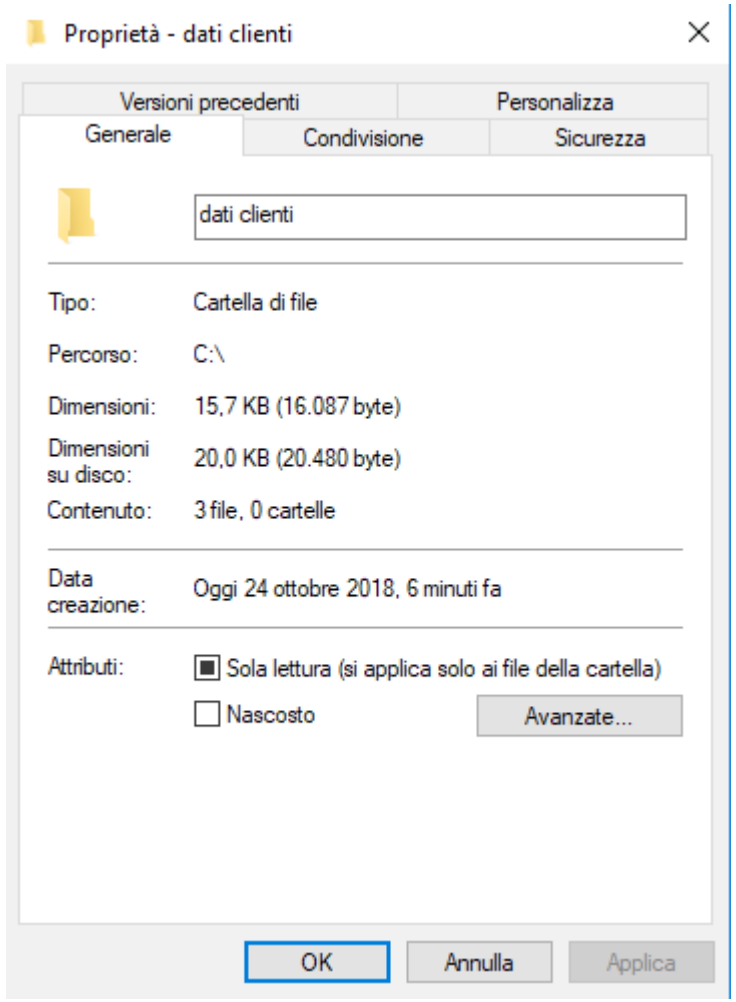


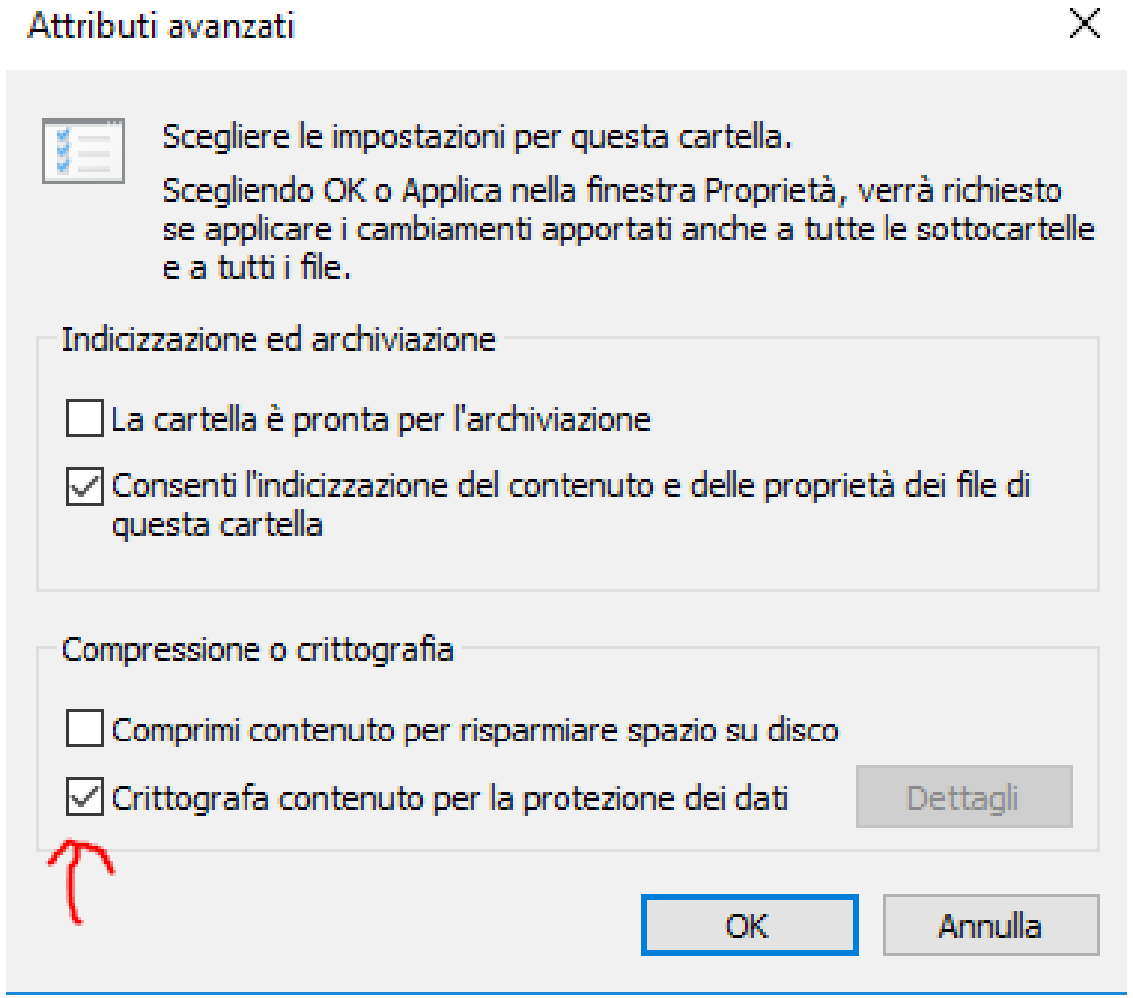
Dati non protetti

MA proteggere l’account utente significa assai poco se qualcuno ha nelle mani il disco fisso (es. di un computer rubato o perso). Accedervi da un altro sistema operativo è facile, e tutti i dati sono leggibili.

I moderni sistemi operativi (in Windows da XP, nell’altamente raccomandabile versione “pro”) hanno **incorporata una criptazione di interi dischi,** w in grado di criptare l’intero contenuto della unità logica. I dati sono decrittati quando l’utente accede al dispositivo (previa autenticazione). Sfortunatamente, non è una caratteristica di solito attiva di default, e richiede una azione per essere attivata.

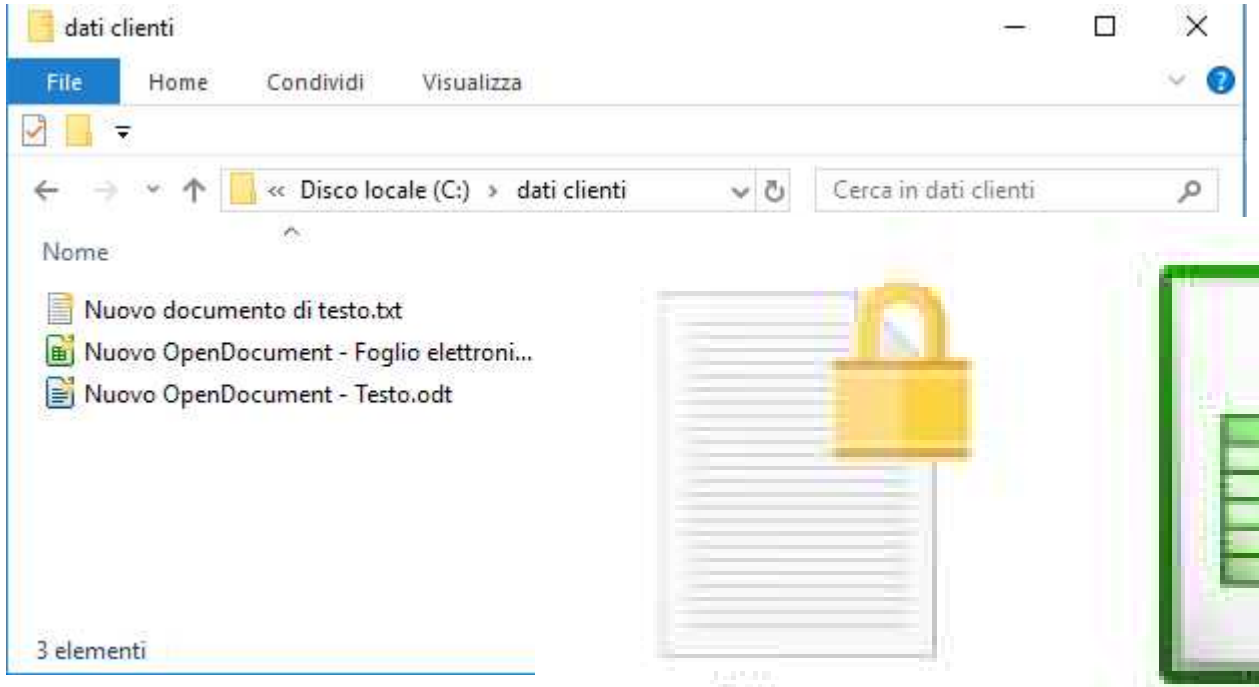
Attivare la criptazione di singole cartelle





Avv. Francesco Tregnaghi - Verona

Attivare la criptazione di singole cartelle

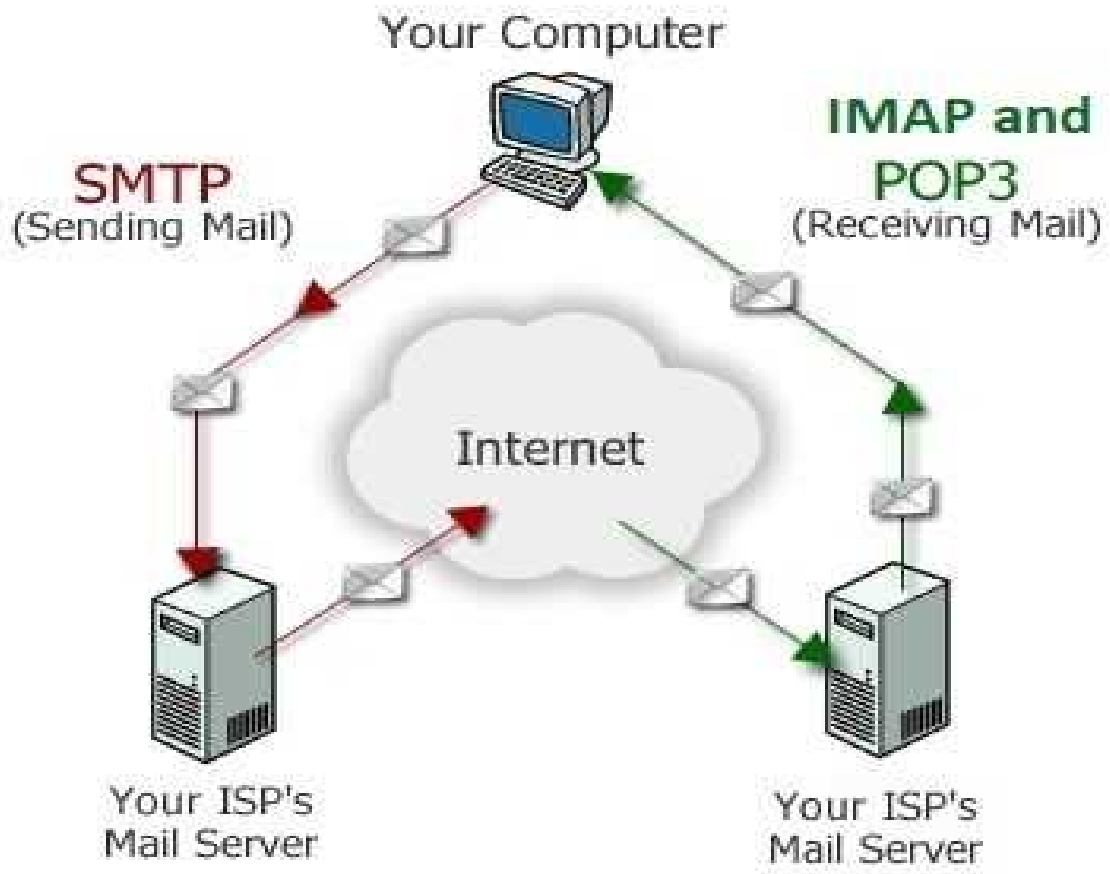


Nuovo documento di testo.txt

Nuovo OpenDocument - Foglio elettronico.ods

Nuovo OpenDocument - Testo.odt

Accesso non sicuro a E-Mail server



POP3, SMTP, IMAP sono protocolll INSICURI

Un buon hacker, da qualsiasi posto, potrebbe leggere le vostre email nello stesso tempo in cui scaricate o caricate i vostri messaggi da/per il server. E leggerne le password per accesso futuro

Gli equivalenti ma crittati protocolli **POP3s, SMTPs, IMAPs** (dove “s” sta per “secure”) devono essere usati al loro posto, in quanto usano un protocollo di buon grado di sicurezza

Passwords troppo semplici

Secondo il produttore del Password manager “Keeper” , la classifica 2016 dell PW più usate era;

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

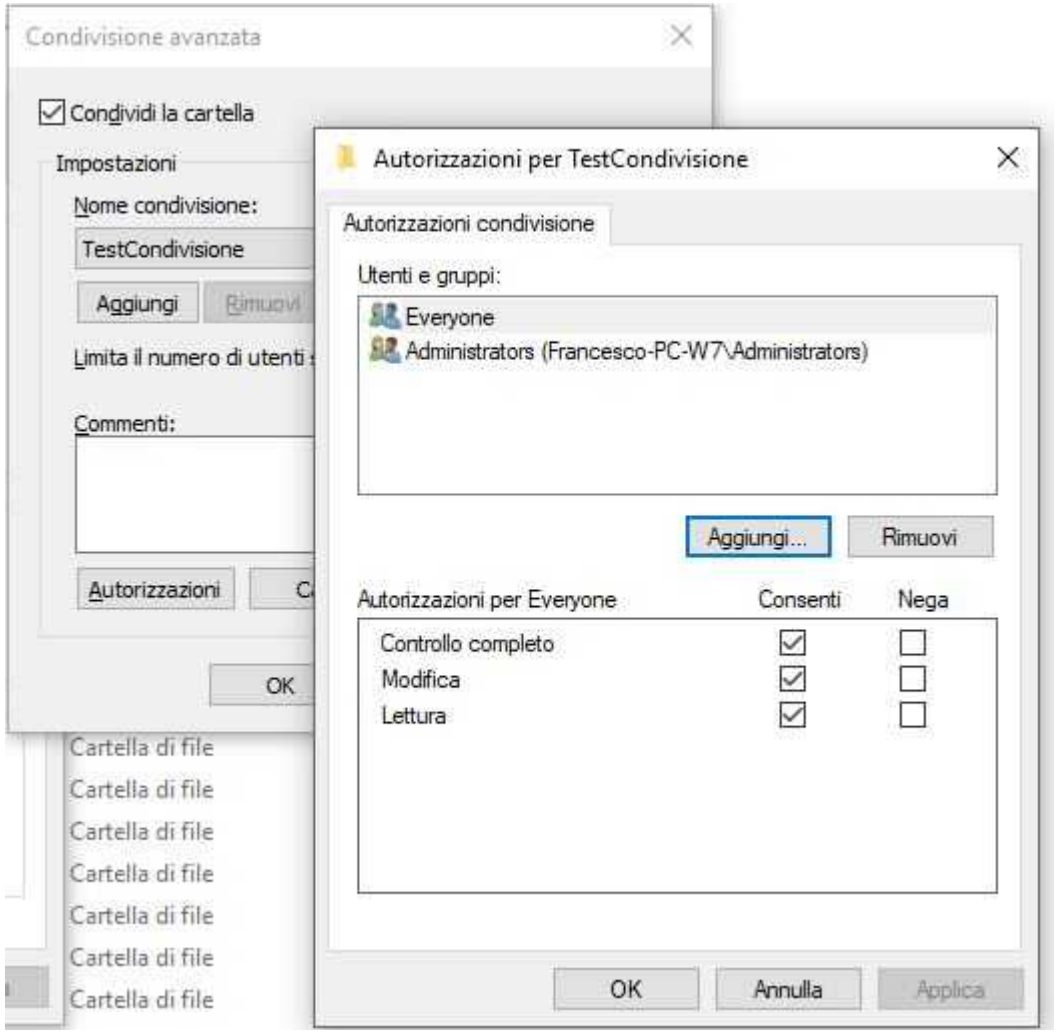
Risorse LAN condivise

Molti piccoli studi condividono la rete locale con colleghi o altri coinquilini, per condividere stampanti, acecsso a internet e altre risorse.

Se la condivisione risorse non è opportunamente settata coi permessi di accesso essa non è controllata, tutti i dati di quella risorsa possono risultare accessibili a persone che non dovrebbero poterle leggere, copiare o distruggere

Ogni risorsa condivisa in tali ambienti deve essere protetta dalle opportune regole di accesso

Settare i permessi di una cartella condivisa



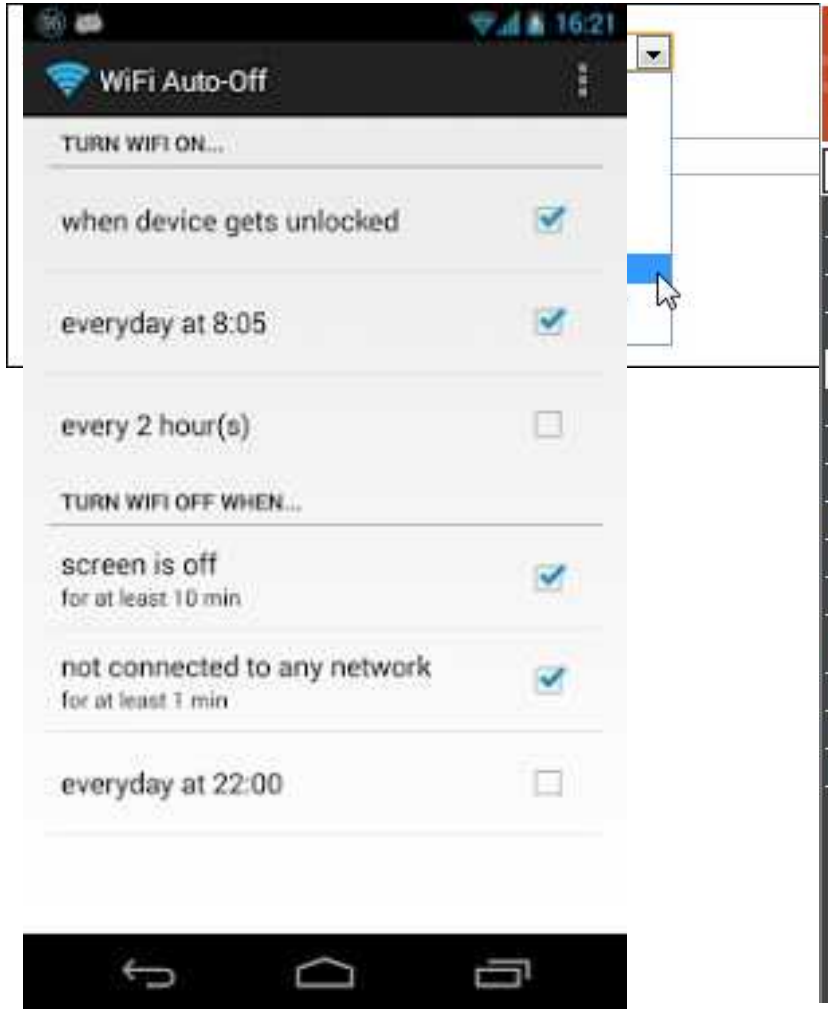
Avv. Francesco Tregnaghi - Verona

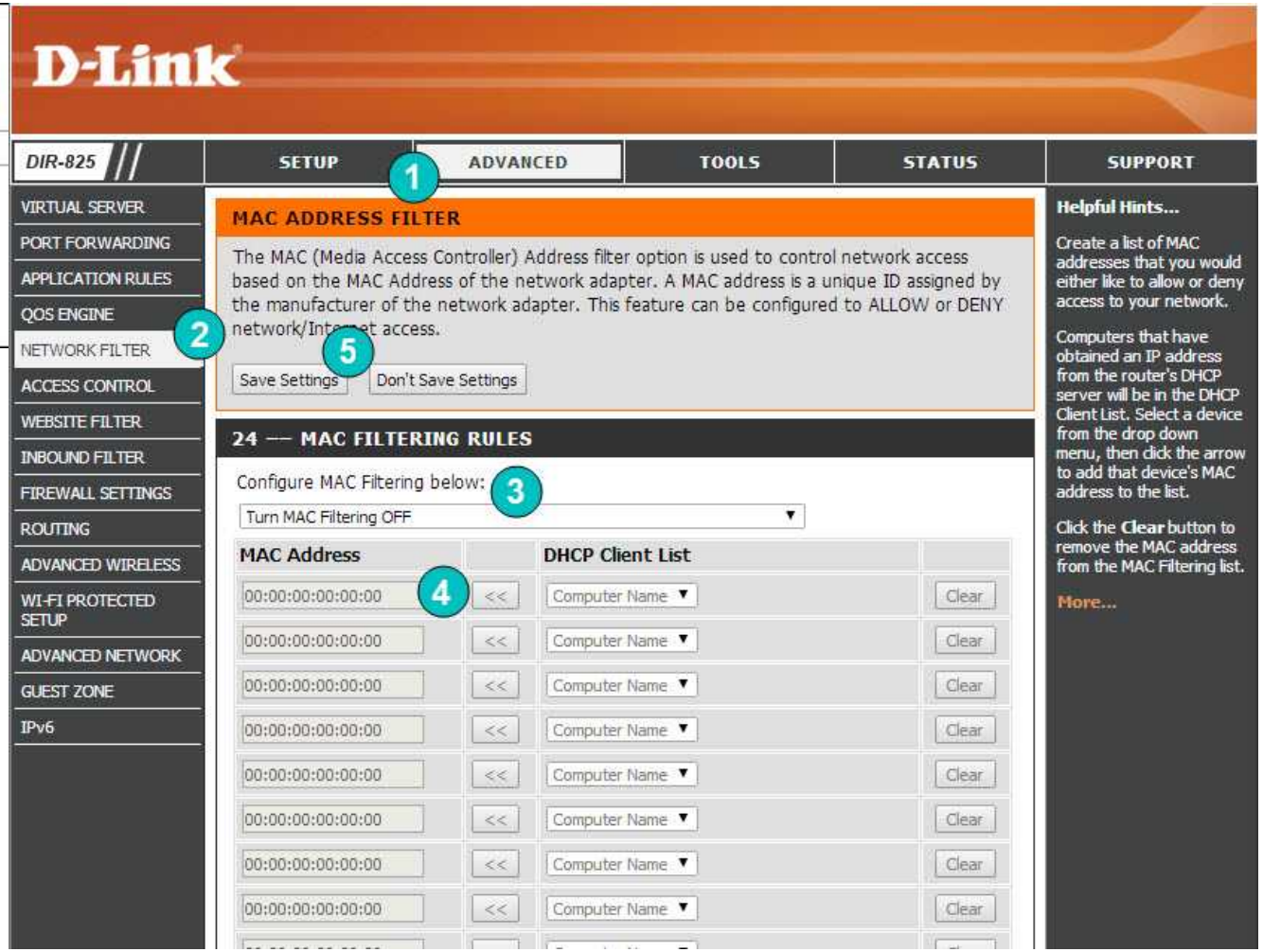
Accesso WiFi alla rete

Accesso WiFi a LAN contenenti dati dovrebbe essere, se necessario:

- Protetto dal protocollo di trasmissione più avanzato
- L'accesso dovrebbe essere limitato a singoli dispositivi, discriminati in base al loro indirizzo MAC
- Spento quando non necessario (molti router WiFi hanno spegnimento/accensione timerati in automatico)

WiFi settings





printer/scanner multifunzione

I moderni scanner di rete hanno dischi rigidi incorporati per archiviare i documenti digitalizzati, che saranno poi prelevati dall'avvocato interessato. Tali file non vengono cancellati automaticamente. Ciò è inaccettabile nelle LAN condivise. Ma, ancor peggio...

In un caso recente, una ditta che ha acquistato una macchina di seconda mano da una società di leasing ha trovato un hard-disk completo di documenti PDF, chiaramente e facilmente identificabili come documenti scansionati da uno studio legale di medie dimensioni di Milano!

Archiviazione Cloud

Il Cloud è fantastico. Possiamo lavorare da tutto il mondo e il backup è assicurato da terze parti ben organizzate. Ce ne sono di eccellenti e gratuiti, ma:

- Il contenuto deve ovviamente essere protetto da una Password “forte”.
- Dovrebbe essere ospitato in UE in quanto il Patriot Act degli Stati Uniti si scontra ancora con l'ambiente UE di protezione dei dati, e memorizzare i dati in un server soggetto ad esso sarebbe una violazione dei regolamenti UE


Cryptolocker 2.0
Your personal files are encrypted
Info
Your important files were encrypted on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.
Encryption was produced using unique public key RSA-4096 generated for this computer. To decrypt files, you need to obtain private key.
The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; the server will destroy the key within 72 hours after encryption completed. After that, nobody and never will be able to restore files.
To retrieve the private key, you need to pay 0.5 bitcoins.
Click proceed to payment to obtain private key.
Any attempt to remove or damage this software will lead to immediate private key destruction by server.
Your files will be lost without payment on:
11/24/2013 3:16:34 PM
See files
<< Back
Proceed to payment >>

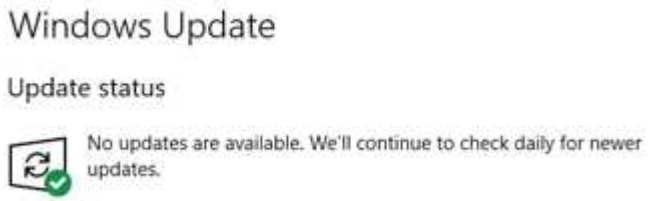
Troyan / Virus threats

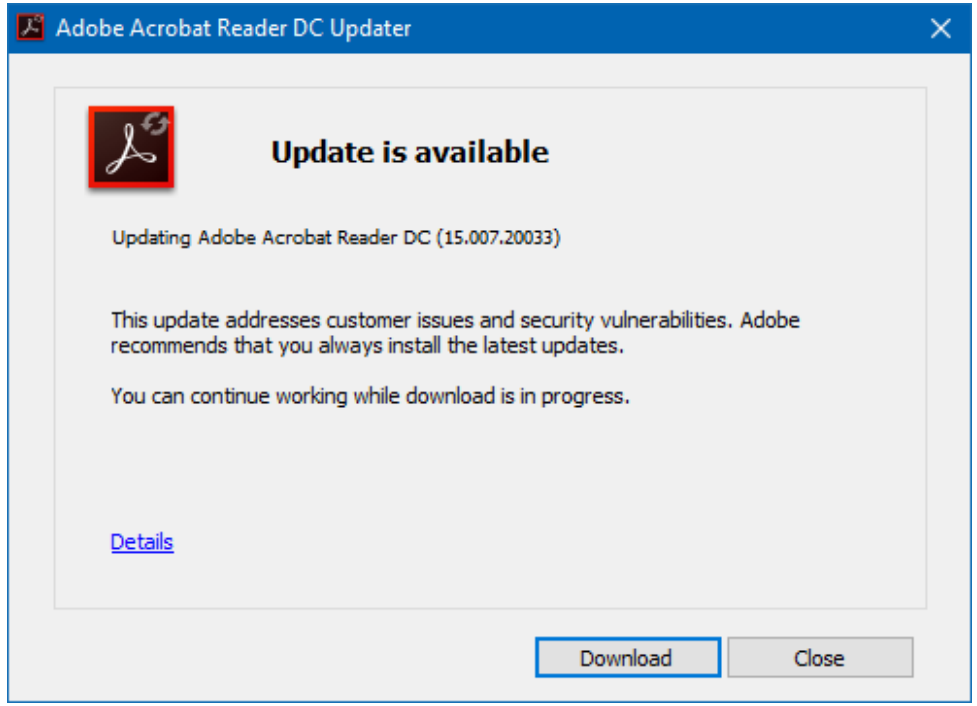
Il c.d. Malware può compromettere sia la sicurezza che la sicurezza ed integrità dei “nostri” dati

- Alcuni sono fatti per rubare “silenziosamente” dati e password.
- Altri (ransomware) non rubano i vostri dati, ma li criptano in blocco (e tutti i backup in tempo reale sono affetti), e promettono la chiave di decrittazione solo se si paga un riscatto. Anche pagando, a volte i dati sono perduti per sempre.
- Un sistema anti-malware/antivirus aggiornato è vitale, as well come anche regole di backup che considerino il rischio che tutte le risorse connesse tra loro sia compromesse allo stesso momento

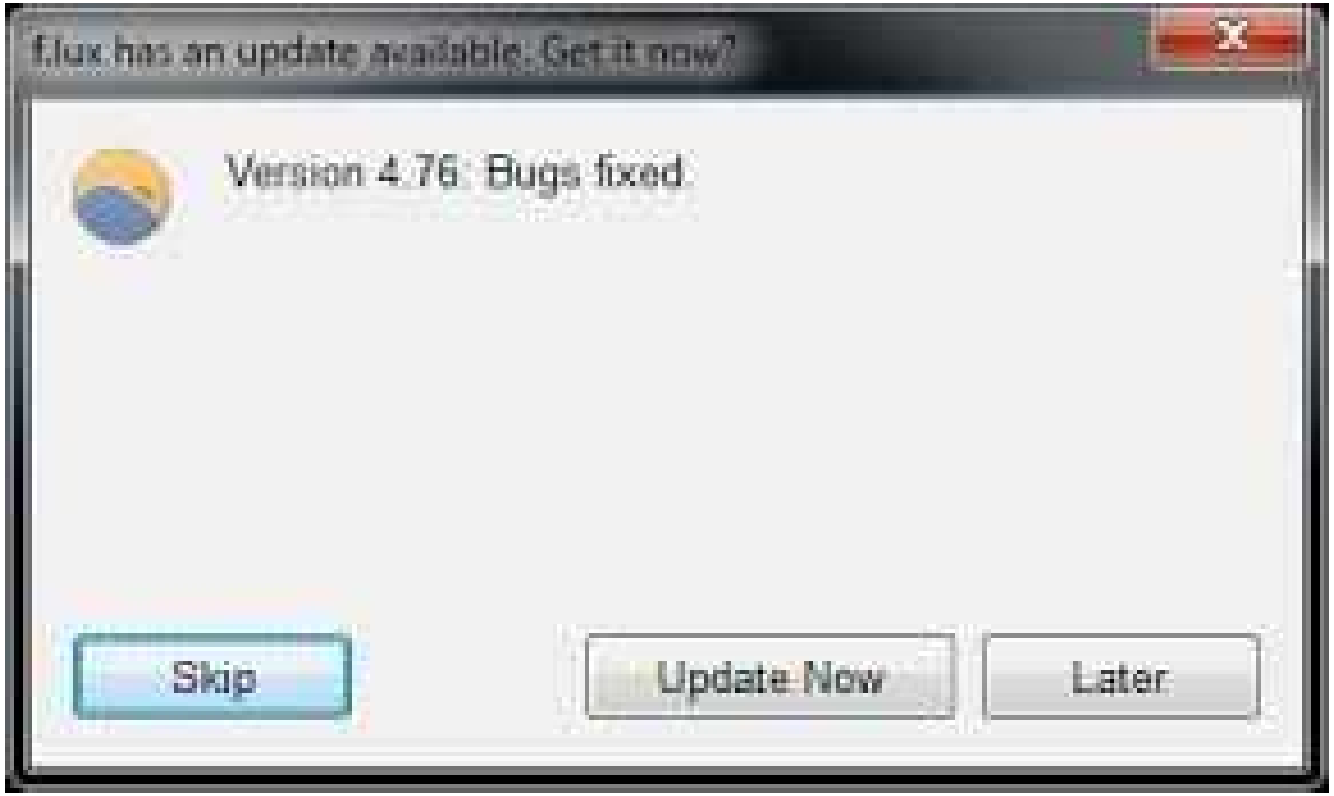
Aggiornamenti Software

- Tutto il software che usiamo, a partire dal sistema operativo e con speciale riguardo al software con accesso a Internet, dovrebbe essere aggiornato all'ultima release, per evitare perdite di sicurezza.





Fallo subito!



Cosa fare?

- Non dobbiamo adagiarci sulle abitudini, ma considerare che le minacce sono in continuo cambiamento, come lo è l'ambiente a cui siamo connessi
- Dobbiamo analizzare il nostro "ambiente digitale" per capirne i rischi concreti.
- Dobbiamo quindi pianificare di conseguenza, per eliminare o ridurre quei rischi
- ...e adeguarci al GDPR!

Come posso capire i rischi che corrono i dati che tratto?

DPIA (Data protection impact assessment, valutazione d'impatto sulla protezione dei dati, Art 35) anche quando non obbligatorio può essere uno strumento molto utile per identificare i rischi

L'autorità francese (www.CNIL.fr) ha sviluppato un software open-source e multi-lingua che può essere uno strumento guidato molto utile per analizzare il nostro ambiente “dati” e identificare i rischi

Ma un avvocato deve diventare un esperto di IT?

- No, certo. Ma un certo grado di preparazione IT è richiesto. Se manca, si può ipotizzare una responsabilità civile o anche deontologica (CCBE guidance 2016)
- Anche se la maggior parte delle azioni da intraprendere per evitare i rischi esposti non è così difficile, un avvocato può utilizzare l'aiuto di un tecnico, MA...
- egli deve conoscere personalmente i rischi e assicurarsi che tutti siano considerati e minimizzati E...
- deve imparare e seguire le buone pratiche nella protezione dei dati nella vita di ogni giorno

Francesco Tregnaghi

Avvocato – Verona, Italy

www.tregnaghi.it

 @Effetiverona

Un ringraziamento a Francesco Paolo Micozzi, del Consiglio dell’Ordine di Cagliari