

UniSIcuri in Rete - Pulizie di primavera

Aprile 2021



Rovistare nella spazzatura: il *trashing*

Sapevate che una delle tecniche di attacco è il *rovistare nella spazzatura*? Il *trashing* consiste nel cercare tra i rifiuti, in particolare quelli cartacei, alla ricerca di informazioni confidenziali e utili. Per quanto possa sembrare disgustoso, *non è un caso* se **nelle aziende dove si trattano dati particolarmente sensibili, come le banche, si utilizzano distruggi documenti e vigono regole stringenti per come vengono gettati i documenti.**

Vi racconto un veloce aneddoto.

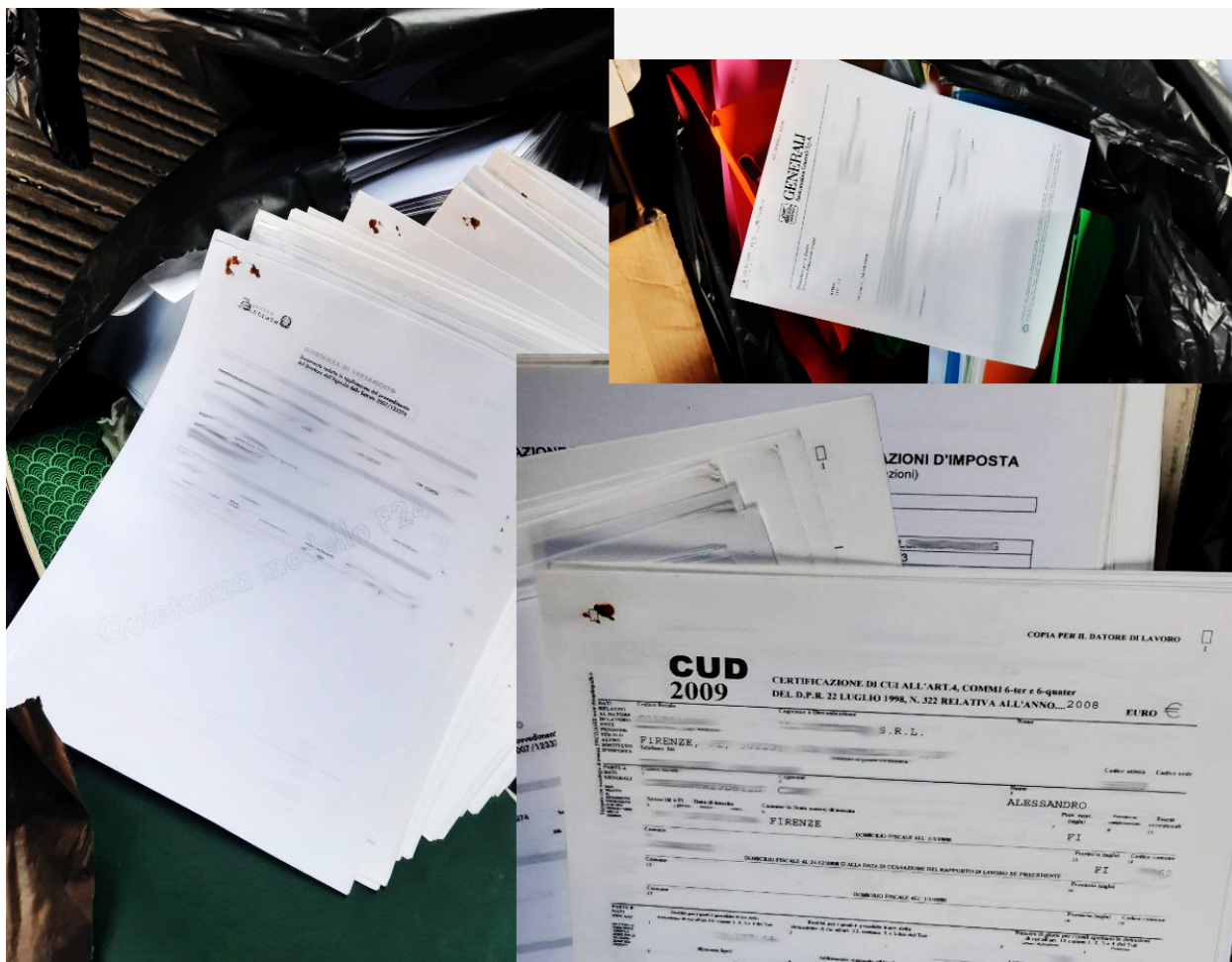
L'altro giorno, mentre stavo raggiungendo l'ufficio, vedo accatastate in un angolo una serie di scatoloni e sacchi neri contenenti fogli e portadocumenti.



Erano le prime ore della mattina e questo mucchio di carta era in attesa del passaggio del camion dell'immondizia ma, nel mentre, questi documenti -tra cui CUD e altri documenti fiscali- erano a disposizione di chiunque passasse da lì.

Con nomi, cognomi, codici fiscali, dati anagrafici, patrimoniali e altre informazioni, questo cumulo di documenti, che ancora non era diventato "spazzatura", rappresentava una vera e propria miniera d'oro di dati!

Chissà, peraltro, cosa ne avrebbero pensato coloro che si son trovati i loro dati fiscali e patrimoniali alla mercé di chiunque passasse da lì...



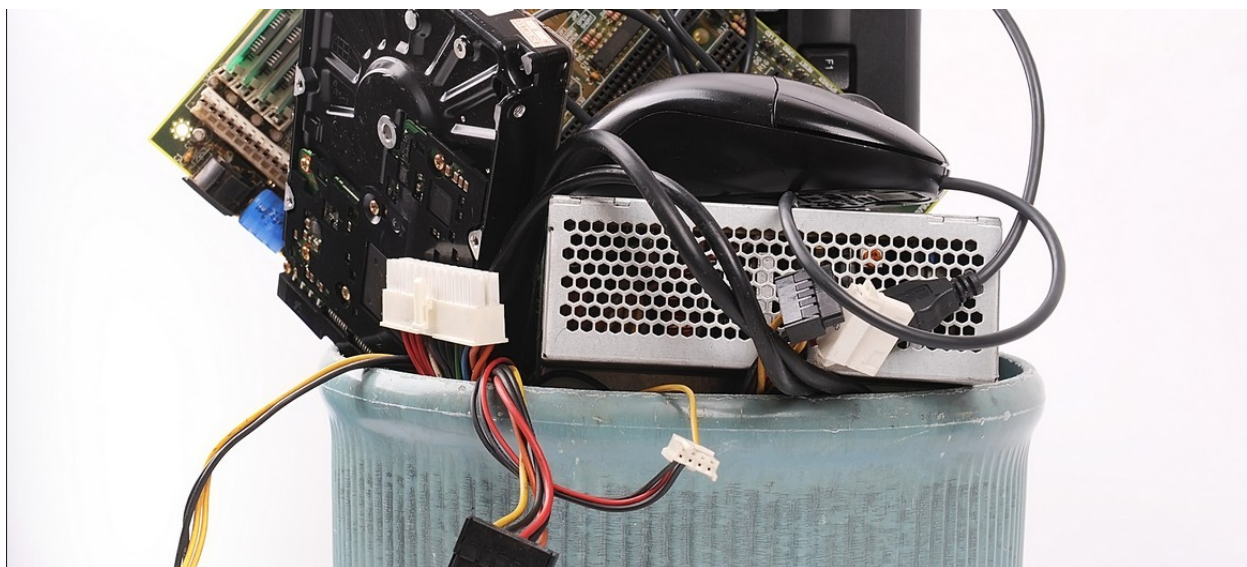
Ciò che buttiamo nell'immondizia, **magari note, appunti, lettere o documenti, potrebbero contenere informazioni sensibili e personali**. Che chiunque, dall'addetto delle pulizie all'operatore ecologico, passando per l'eventuale curioso che passa per strada proprio accanto al mucchio dei documenti in attesa di essere smaltiti, potrebbero recuperare e utilizzare a proprio favore.

Non parliamo ovviamente solo di documenti cartacei: **particolare attenzione va fatta quando gettiamo i nostri dispositivi informatici, dal computer ai CD alle schede di memoria**, che se non adeguatamente "ripuliti" prima dello smaltimento, potrebbero essere recuperati insieme ai dati che contengono.

👉 Assicuriamoci di **cancellare adeguatamente i dati personali e sensibili** su tutto ciò che buttiamo nell'immondizia!

Per difendersi da questo tipo di attacchi è necessario **fare sempre attenzione a ciò che gettiamo via**, assicurandoci di aver adeguatamente distrutto e reso irrecuperabili eventuali informazioni personali e confidenziali.

Per quanto riguarda **i dispositivi elettronici di memorizzazione dati**, come hard disk e chiavette e schede USB, si può utilizzare uno dei tanti programmi per il “wiping” sicuro. **Limitarsi a cancellare i files spesso non è sufficiente**: molti sistemi operativi non cancellano realmente i files “cancellati”, limitandosi a marcarli come tali ma mantenendoli comunque recuperabili attraverso specifici software anche di pubblico dominio (come *TestDisk & PhotoRec*¹).



Per quanto riguarda **supporti come CD-ROM e DVD**, la **distruzione fisica prima di gettarli è la soluzione migliore** per scongiurare il recupero: spezzarli, tagliarli o grattare la superficie leggibile (*facendo attenzione a non ferirsi!*).

¹ https://www.cgsecurity.org/wiki/TestDisk_Download

La crittografia², in ogni caso, è nostra amica: attivare la **cifratura automatica del disco rigido³** e dei supporti, usando una **password ragionevolmente robusta⁴**, garantisce che in caso di furto, smarrimento o “getto nell'immondizia”, i nostri dati siano al sicuro da occhi indiscreti.

Per finire ricordo che il GDPR individua come “*data breach*” qualsiasi “*violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali*”.

Shouldersurfing

Un'altra tecnica di attacco utilizzata è lo *shouldersurfing*, ovvero lo “sbirciare da dietro le spalle”, magari proprio mentre digitiamo la password di accesso al PC, il PIN del bancomat o il codice di sblocco dello smartphone.

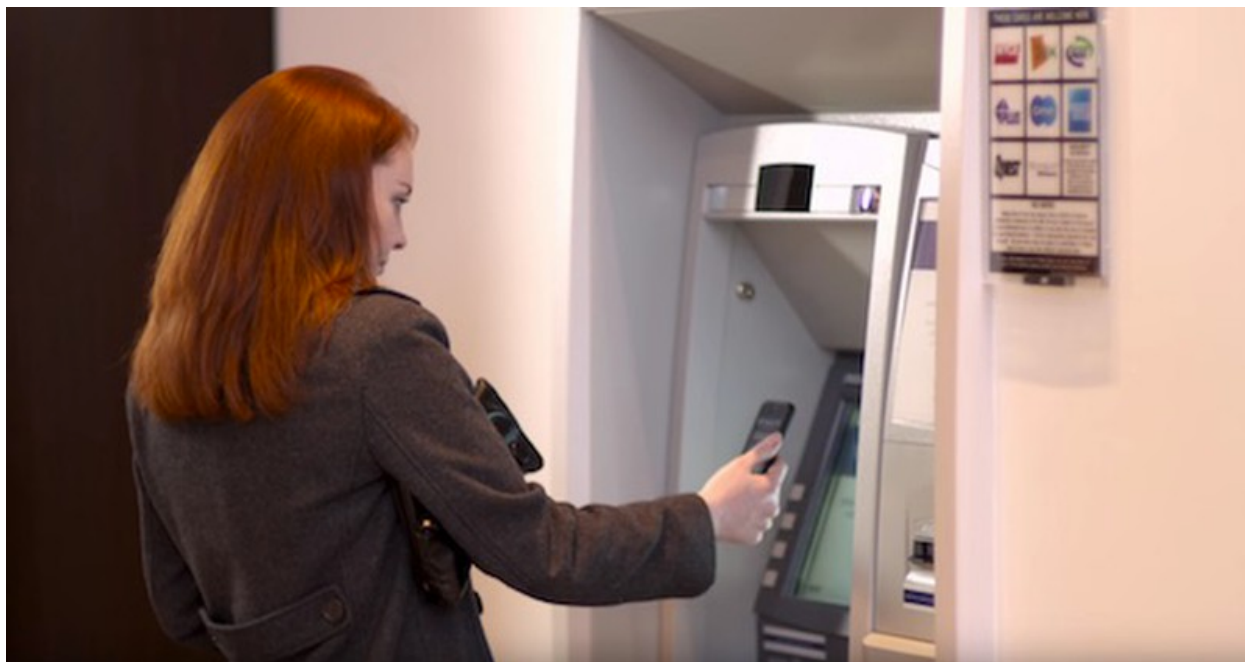


² <https://www.veracrypt.fr/code/VeraCrypt/>

³ <https://docs.microsoft.com/it-it/windows/security/information-protection/encrypted-hard-drive>

⁴ <https://howsecureismypassword.net/>

E' una tecnica che richiama alla mente gli anni della scuola, quando magari sbirciavamo sul compito della compagna o del compagno più bravo, cercando magari di carpirne qualcosa di utile: analogamente, **lo sbirciare da parte di sconosciuti, se non facciamo attenzione, può esporci ad alcune sgradevoli conseguenze.**



Avete notato, ad esempio, che agli sportelli ATM ("Bancomat") sono presenti, sopra il monitor, due specchietti curvi? Servono per consentirci di controllare, senza doversi necessariamente voltare e perdere di vista il monitor, se qualcuno sta alle nostre spalle a guardare ciò che facciamo, in particolare quando digitiamo il PIN.

Anche alcune **pellicole per il display dello smartphone o del tablet**, che limitano la visualizzazione solamente a chi sta davanti (chiamate "*privacy shield*"⁵), possono aiutare a evitare che qualcuno "sbirci" mentre digitiamo un PIN, una password o leggiamo gli SMS.

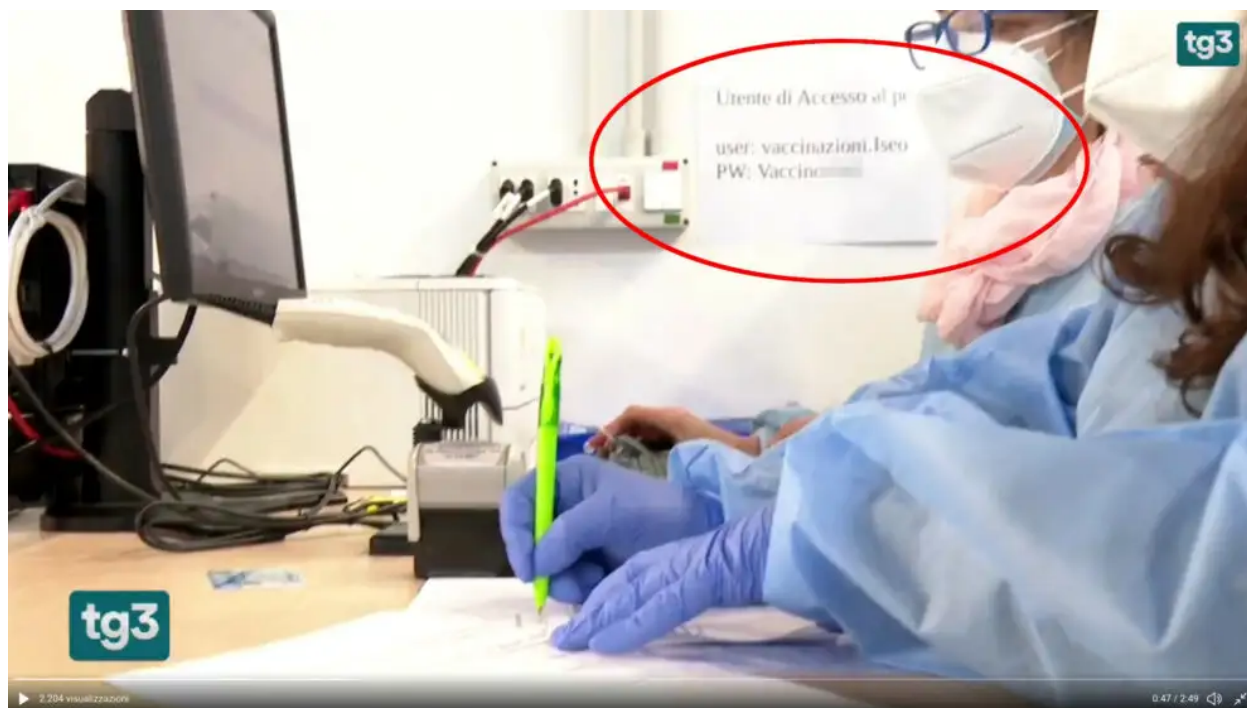
Per finire, **mai e poi mai dare la propria password per telefono, per chat, per e-mail** o qualsiasi altro canale: nessuno dovrà mai chiedervela legittimamente e quasi sicuramente dietro la richiesta si nasconde una truffa.

⁵ <https://www.amazon.it/s?k=privacy+shield>

👉 Mai, per alcun motivo, dare la propria password o PIN di accesso ai servizi on-line!

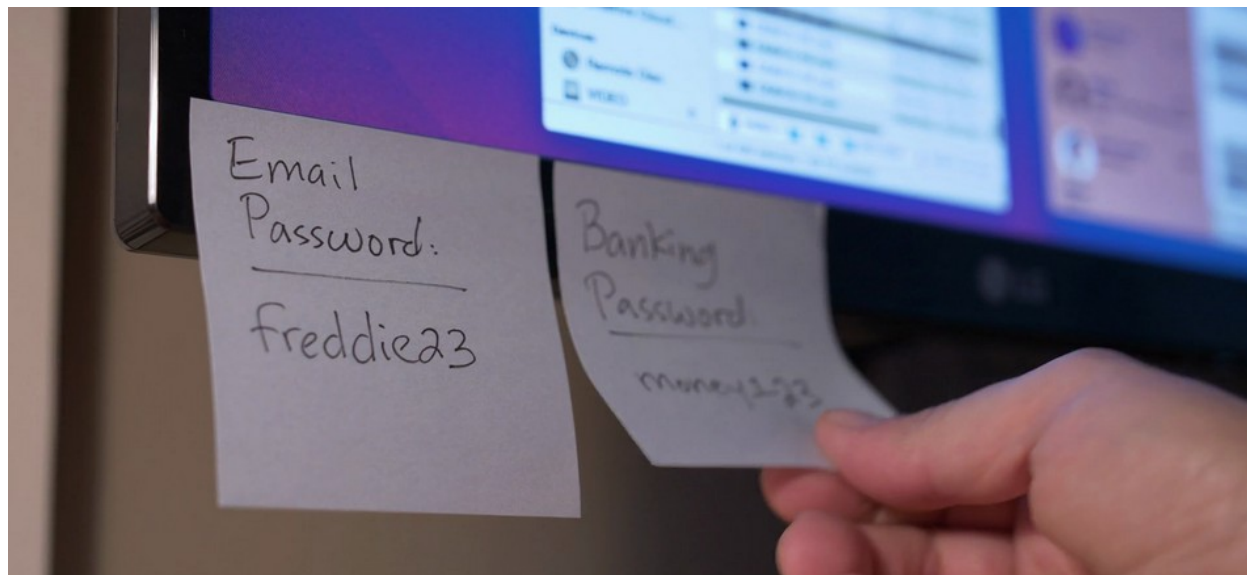
Post-it e altre gaffe

Una delle ultime “gaffe” è avvenuta pochi mesi fa, durante un servizio sulle vaccinazioni CoVID: **per qualche istante, su milioni di teleschermi è apparsa l'immagine di un foglio A4 attaccato alla parete dove campeggiavano, in bella vista, username e password per l'accesso ai PC.**



Il clip, trasmesso dal TG3 regionale, è finito anche sul web, esponendo al “*pubblico ludibrio*” l'istituto dove si è verificata questa indebita esposizione di credenziali.

Al di là della vicenda, che si unisce ad altre ben più gravi (*una simpatica rassegna potete trovarla qui: [Four embarrassing password leaks on live TV](#)⁶*), questo dimostra come **l'abitudine di scrivere le password -o altre informazioni sensibili e personali- su post-it o fogli attaccati a monitor o al muro sia decisamente da evitare.**



Soprattutto per gli uffici destinati ad accesso pubblico, il rischio che le credenziali possano essere copiate ("perdita di esclusività") è concreto ed espone a potenziali attacchi.

Così come non dobbiamo scrivere il PIN del Bancomat sul fogliettino che teniamo nel portafoglio o scrivere l'indirizzo di casa sul portachiavi, **custodire adeguatamente protette le credenziali di accesso ai servizi e portali on-line è un obbligo** anche normativo.

Mercato dell'usato

Può sembrare strano ma **il mercato dell'usato dei dispositivi elettronici, smartphone in testa, è una miniera d'oro di dati personali** sostenuto dagli utenti che, per pigrizia o ignoranza, **non cancellano correttamente** i dispositivi che rivendono.

⁶ <https://www.itgovernance.co.uk/blog/four-embarrassing-password-leaks-on-live-tv>



Prima di cedere, rivendere o gettare uno *smartphone* (ricordatevi che si tratta di rifiuti RAEE e vanno smaltiti nel modo corretto!) o un PC, bisogna sempre assicurarsi di aver rimosso correttamente e completamente i dati che contiene:

1. **rimuovere tutte le schede di memoria** (*miniSD*), *hard-disk* o altre periferiche di memorizzazione;
2. **effettuare il ripristino alle impostazioni di fabbrica**: cancellare solo le app o la rubrica non è sufficiente a eliminare le informazioni personali;
3. **assicurarsi di aver rimosso qualsiasi informazione personale**: anche se lo regaliamo a un amico o un parente, non possiamo mai sapere dove potrebbe andare a finire nel futuro;

Riferimenti normativi

La normativa europea sulla protezione dei dati personali ("GDPR") impone **la definizione di contromisure atte a minimizzare la possibilità del furto di dati** ("*data breach*") e le eventuali conseguenze.

La Rete Internet è diventata strumento indispensabile per l'espletamento di gran parte delle attività lavorative dell'Ateneo. Attraverso la Rete, l'Ateneo permette agli studenti, ai docenti, ai ricercatori, ai tecnici, agli amministrativi, ai collaboratori e a tutto il restante personale, l'accesso ai dati e ai servizi necessari allo svolgimento delle attività didattiche e amministrative. **La sicurezza dei dati e delle infrastrutture assume, pertanto, un ruolo essenziale per le libertà e i diritti degli interessati e per il mantenimento della *business continuity*.**

Qualsiasi dispositivo connesso in Rete diventa attore del processo di business e deve rispettare alcuni requisiti minimi per la salvaguardia dell'infrastruttura ICT e dei suoi servizi.

- **Garante per la protezione dei dati personali** - Regolamento europeo in materia di protezione dei dati personali - www.garanteprivacy.it/regolamentoue
- **Istruzioni pratiche per una cancellazione sicura dei dati: le raccomandazioni degli operatori** - www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1574080
- **Agenzia per l'Italia digitale** - Misure minime di sicurezza ICT per le PA - www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

Contatti e siti web utili

- Gestione delle **credenziali unisiPass** e **aggiornamento password**: my.unisi.it
- **Avvisi di sicurezza** dell'Università di Siena: www.uet.unisi.it/category/sicurezza/
- Servizio di **assistenza tecnico-informatica** dell'Università degli Studi di Siena: helpdesk@unisi.it
- Segnalazione **violazioni al trattamento dei dati personali**: abuse@unisi.it