I ISTRUZIONI
O OPERATIVE
P PRIVACY

REDATTO AI SENSI E PER GLI EFFETTI DELL'ART. 29 REL REGOLAMENTO U.E. 2016/679 AL FINE DI ISTRUIRE GLI AUTORIZZATI AL TRATTAMENTO CIRCA LE MODALITA' DELLO STESSO.

COMPLETO DI:

PRINCIPI BASE DI IGIENE INFORMATICA

MODELLO REV. 2022

STUDIO TECNICO LEGALE
CORBELLINI
Studio AG.I.COM. S.r.l.

Redatto a cura e negli uffici del D.P.O. :

STUDIO AG.I.COM. S.R.L. UNIPERSONALE
Via XXV Aprile, 12 – 20070 SAN ZENONE AL LAMBRO (MI)
Tel. 02 90601324 Fax 02 700527180 info@agicomstudio.it

www.agicomstudio.it

SCOPO DEL PRESENTE MANUALE

E' da precisare in premessa che le presenti Istruzioni Operative Privacy (I.O.P.), costituiscono parte integrante della lettera di autorizzazione che ha ricevuto in qualità di soggetto che opera all'interno dell'Istituto Scolastico e che quindi è necessitato a trattare dati personali al fine di svolgere correttamente le mansioni previste dal proprio profilo professionale.

Con la locuzione "istruzioni operative" intendiamo una raccolta di obblighi, indicazioni, procedure e divieti, presentata al fine di ottemperare all'obbligo di cui all'Art. 29 del Regolamento U.E. 2016/679: "*Il responsabile del trattamento o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali, non può trattare tali dati se non è stato istruito in tal senso dal titolare del trattamento…"*.

Questo manuale viene messo nella disponibilità di tutti gli autorizzati ed inoltre viene utilizzato come testo di riferimento in occasione dei corsi di formazione che devono essere svolti all'interno dell'Istituto.

Ma qual è lo scopo ultimo che si prefigge l'Istituto fornendo queste istruzioni operative?
Semplificando, ma non troppo, possiamo dire che tutte le istruzioni contenute in questo documento si prefiggono l'obiettivo di scongiurare che dati personali appartenenti ad allievi, dipendenti o fornitori dell'Istituto, vengano divulgati e quindi posti nella disponibilità di chi non è autorizzato a conoscerli (in altre parole l'obiettivo di tutelare la loro privacy).

DEFINIZIONI

Perché tutti possano comprendere al meglio quanto scritto nel presente manuale, prendendo spunto dall'articolo 4 del Regolamento UE 2016/679 (GDPR), diamo alcune definizioni di base:

Dato anonimo / personale: Si parla di "dato personale" quando ci troviamo di fronte ad una informazione riferibile ad una persona fisica identificabile (ad es. Mario Rossi di 3C ha i capelli biondi), mentre se l'informazione non fa riferimento a nessuno nello specifico (p.es. il 30% degli allievi che frequentano l'Istituto ha i capelli biondi) allora siamo di fronte ad un dato anonimo.
Le normative sulla privacy, dalla loro nascita a tutt'oggi, tutelano solo ed esclusivamente i dati personali.
E' chiaro a tutti che il livello di tutela richiesto dipende non solo dal fatto che il dato sia personale, ma anche dalla delicatezza dell'informazione.
Una informazione come "*essere diversamente abile*" è ovviamente molto più delicata rispetto ad "*avere i capelli biondi*" e quindi la normativa ha introdotto diverse gradazione al concetto di dato personale: il dato comune, il dato particolare ed il dato giudiziario.

Dato comune / particolare / giudiziario: Un dato personale si dice "particolare" quanto fa riferimento: allo stato di salute, all'orientamento sessuale, all'orientamento politico o alla fede religiosa di un soggetto. Si parla inoltre di dato particolare quando si tratta di informazioni genetiche (D.N.A. etc.) o biometriche (impronte digitali etc.).
Con il termine "dato giudiziario" invece si intendono i precedenti penali ed i carichi pendenti di un soggetto, ossia i suoi trascorsi giudiziari. Tutti i dati che, pur essendo personali, non rientrano nelle definizioni sopra date (anagrafici, andamento scolastico, importo dello stipendio, orari etc.) si definiscono "dati comuni".
E' bene precisare che, anche i dati comuni, in quanto dati personali, sono tutelati ma con una intensità minore rispetto a quanto non sia previsto per i dati particolari e giudiziari.

Trattamento: senza scomodare la definizione di legge, possiamo ben dire che costituisce un trattamento di dato personale qualsiasi operazione io svolga con un dato personale (raccolta, registrazione, organizzazione, trasmissione, cancellazione etc.) anche la mera detenzione.
Questo significa che la sola custodia all'interno della nostra borsa di un foglietto riportante il numero di telefono di un allievo o la memorizzazione del medesimo numero sul nostro telefono, costituisce un trattamento di dato personale ed è quindi regolamentato dalla legge.
Nel primo caso (foglietto in borsa) saremo di fronte ad un trattamento di dato in formato cartaceo, nel secondo caso (memorizzazione nel telefono) in formato digitale.

Titolare del Trattamento: E' l'Istituto Scolastico, incarnato nella persona che ne ha la rappresentanza legale. Nel caso delle Scuole Statali, tale incarico è del Dirigente Scolastico, mentre per le Scuole Paritarie, dipende dalla loro forma giuridica (società, cooperativa, ente etc.).

Autorizzato al Trattamento: Partendo dal presupposto che il Titolare del Trattamento, da solo, non può portare avanti l'intera attività scolastica, tutti i suoi collaboratori interni che lo affiancano nell'attività (Segreteria, Docenti, Collaboratori Scolastici, Assistenti Tecnici etc.) sono da considerarsi "Autorizzati al Trattamento".
Naturalmente non tutte le autorizzazioni hanno lo stesso perimetro, esistono autorizzazioni molto ampie (Collaboratore vicario, D.S.G.A., Segretario Generale etc.), altre più ridotte (Docente che presta servizio in 2B, Assistente Amministrativo etc.) ed altre ancora solo eventuali (Collaboratore Scolastico, Ausiliario, Tecnico etc.).
Il perimetro dell'autorizzazione è evidenziato nella lettera di autorizzazione a cui il presente manuale è allegato.

Responsabile del Trattamento: Il concetto è affine a quello sopra definito di autorizzato, cambia il fatto che il responsabile è normalmente un soggetto esterno (che quindi non ha un contratto di lavoro con la scuola), con una propria organizzazione autonoma, a cui l'Istituto attribuisce compiti di trattamento dati (gestore del registro elettronico, della segreteria digitale, tesoreria, RSPP, DPO, Medico Competente etc.).
In questo caso la sua designazione avviene mediante un vero e proprio contratto.

ADEMPIMENTI GENERALI

Apriamo elencando alcune regole generali valide per tutti:

- rispettare i principi generali del GDPR, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi, è vietato trattare i dati in modo diverso rispetto a quanto previsto dalle procedure interne;

- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;

- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti dell'azienda/ente;

- rispettare le misure di sicurezza adottate, atte a salvaguardare la riservatezza e l'integrità dei dati;

- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;

- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;

- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;

- mantenere riservate le proprie credenziali di autenticazione;

- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;

- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;

- informare senza ritardo il proprio responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;

- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;

- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

ISTRUZIONI OPERATIVE

All'interno dell'Istituto Scolastico, al fine di scongiurare ogni violazione di dati personali, tutti gli Autorizzati al Trattamento dei dati sono tenuti ad adottare le seguenti misure di sicurezza:

MISURE DI SICUREZZA DI NATURA TECNICA

Queste misure di sicurezza sono rivolte a tutti i soggetti autorizzati che siano anche utenti informatici (ossia che abbiano a disposizione delle credenziali per l'accesso ad una o più reti, locali o remote, di Istituto).
Si precisa che, all'interno delle regole che seguono, talvolta si fa riferimento genericamente al "servizio tecnico" quale riferimento per ogni questione di natura informatica; Con tale termine si intende il soggetto interno o esterno a cui ordinariamente l'Istituto si rivolge per la gestione e la manutenzione del sistema informatico.

MISURA DI SICUREZZA	RISCHIO CONTRASTATO
La parola chiave (password) relativa all'utenza creata per Lei per accedere alle reti, locali o remote, di Istituto, deve essere custodita con grande cura in modo da scongiurare che possa venire nella disponibilità di altri soggetti. E' vietato utilizzare password eccessivamente banali (data di nascita, nome del figlio etc.), devono essere complesse, formate da almeno 8 caratteri e costituite almeno da una lettera maiuscola, una minuscola ed un numero.	**ACCESSO AI DATI DIGITALI DA PARTE DI SOGGETTI NON AUTORIZZATI**
Le parole chiave (password) devono essere modificate al primo accesso dopo la loro consegna e poi con una frequenza trimestrale.	
E' vietato comunicare, anche se richiesta, la password personale a chiunque. Se questo dovesse accadere per questioni di natura tecnica, è necessario modificarla immediatamente dopo.	
E' vietato collocare file contenenti dati personali, in qualsiasi formato, in aree (cartelle) comuni accessibili a chiunque, in tali aree è consentito salvare esclusivamente documenti anonimi quali la modulistica.	
E' vietato utilizzare chiavette o altri device personali sui sistemi informatici scolastici prima di aver eseguito una scansione antivirus degli stessi.	**DISTRUZIONE E CONSEGUENTE PERDITA DEI DATI**
E' vietato trasferire dati personali di natura particolare o giudiziaria tramite e-mail in chiaro, ossia senza averli preventivamente criptati (protetti con password) ed aver trasmesso la password mediante una altro canale (altra e-mail, telefonata etc.).	**COMUNICAZIONE INDEBITA DI DATI PERSONALI**
E' vietato utilizzare drive o cloud o altri strumenti che non siano espressamente autorizzati dal Titolare del Trattamento per collocare dati personali riferibili ad interessati (allievi, dipendenti, fornitori). Per il collocamento dei dati è necessario che il Titolare intrattenga un rapporto contrattuale con il soggetto gestore del servizio remoto.	
I supporti informatici contenenti dati personali (chiavette, dischi removibili etc.), prima della loro dismissione, devono essere trattati in modo che tali dati non siano in alcun modo recuperabili (formattazione a basso livello dei dischi o distruzione fisica).	
Tutti i supporti magnetici rimovibili (chiavette USB, dischi etc.) contenenti dati particolari e giudiziari, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati, ciascun utente potrà contattare il personale del Servizio Tecnico (interno od esterno) ed seguire le istruzioni da questo impartite per la loro distruzione. In ogni caso, i supporti magnetici contenenti dati particolari o giudiziari devono essere dagli utenti adeguatamente custoditi in armadi chiusi o, in alternativa, criptati mediante impiego di password L'utente è responsabile della custodia dei supporti e dei dati in essi contenuti.	**USO IMPROPRIO DI SUPPORTI REMOVIBILI**

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. È fatto divieto di utilizzare le caselle di posta elettronica ufficiali per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per: l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa; l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list; la partecipazione a catene telematiche (o di Sant' Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Servizio Tecnico e non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. È obbligatorio porre la massima attenzione nell'aprire gli allegati di posta elettronica, non eseguire download di file eseguibili o documenti da siti Web o FTP non conosciuti. Sarà comunque consentito al Titolare del trattamento o persona da lui individuata, di accedere alla casella di posta elettronica dell'utente per ogni ipotesi rilevante ed urgente per cui si renda necessario.	**USO IMPROPRIO DELLA POSTA ELETTRONICA**
Il PC, laptop o notebook, assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo che tale comportamento, durante l'orario di lavoro, sia espressamente autorizzato dal Titolare del Trattamento. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per: l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione; l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Titolare del trattamento e comunque nel rispetto delle normali procedure di acquisto; ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa; la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Titolare; Gli eventuali controlli, compiuti dal personale incaricato dal Titolare del Trattamento del Servizio Tecnico, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.	**USO IMPROPRIO DI INTERNET**

MISURE DI SICUREZZA DI NATURA COMPORTAMENTALE

Queste misure di sicurezza sono rivolte, in generale, a tutti i soggetti autorizzati.

MISURA DI SICUREZZA	RISCHIO CONTRASTATO
I dati personali detenuti in formato cartaceo, devono essere custoditi all'interno di cassetti, schedari o armadi chiusi a chiave.	**ACCESSO AI DATI DA PARTE DI SOGGETTI NON AUTORIZZATI**
La chiave dei cassetti, schedari o armadi in cui vengono custoditi i dati personali in formato cartaceo deve essere detenuta in via esclusiva da coloro che hanno l'autorizzazione a poter trattare quei dati.	
E' vietato a tutto il personale che non ne abbia titolo specifico, l'accesso ai locali di direzione, segreteria, CED ed agli archivi, in assenza di un operatore autorizzato.	
Il personale che presta servizio nei locali di direzione, segreteria, CED ed agli archivi, quando esce dagli stessi e si accorge di essere l'ultimo, si preoccupa della loro chiusura a chiave salvo che i dati personali in essi contenuti non siano resi inaccessibili mediante la loro collocazione all'interno di cassetti, schedari e armadi chiusi a chiave ed elaboratori protetti da password.	
E' vietato trasferire dati personali di natura particolare o giudiziaria tramite semplici fogli che non siano celati all'interno di buste, cartellette o altri contenitori che consentano il loro occultamento.	**COMUNICAZIONE INDEBITA DI DATI PERSONALI**
I documenti cartacei contenenti dati personali, al momento della loro dismissione, devono essere distrutti mediante impiego di distruggidocumenti o finemente triturati anche mediante metodi manuali.	
E' vietata la comunicazione di ogni dato personale al di fuori dei casi in cui la stessa sia espressamente prevista dalla legge o prevista dall'organizzazione scolastica.	
L'utente è responsabile di ogni device (PC, tablet, smartphone etc.) assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. Quando gli stessi sono utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni sia ai dati che al device stesso.	**SOTTRAZIONE E SMARRIMENTO DEI DEVICE SCOLASTICI**
I dati personali possono essere forniti a chi non è autorizzato a conoscerli anche con la modalità più semplice del mondo ossia parlando ad alta voce con chi è autorizzato a conoscerli, senza preoccuparsi del fatto che qualcuno nelle vicinanze li possa indebitamente ascoltare. Per questo motivo, l'autorizzato deve avere cura di tenere un tono di voce adeguato all'argomento che viene trattato quando parla al telefono o durante i colloqui individuali o ancora nell'attività di sportello.	**ASCOLTO DI DATI PERSONALI DA PARTE DI SOGGETTI NON AUTORIZZATI**

DATA BREACH

Queste misure di sicurezza sono rivolte, in generale, a tutti i soggetti autorizzati, nel momento in cui vengono a conoscenza di una violazione di dati personali, commessi da loro stessi o da altri.

MISURA DI SICUREZZA	RISCHIO CONTRASTATO
Quando si verifica una violazione di dati personali, il Titolare del trattamento, entro 72 ore, deve darne notizia all'Autorità Garante per la protezione dei dati, notificando quella che, nella terminologia del G.D.P.R., si chiama "*data breach*" che in italiano significa "breccia nei dati". Chiunque si renda conto di una violazione deve pertanto darne immediata comunicazione al Titolare del Trattamento.	**MANCATA O RITARDATA NOTIFICA AL GARANTE DELLA VIOLAZIONE**

COME DIFENDERCI DAI RISCHI CONNESSI ALL'UTILIZZO DI DEVICE ?

PRINCIPI BASE DI IGIENE INFORMATICA

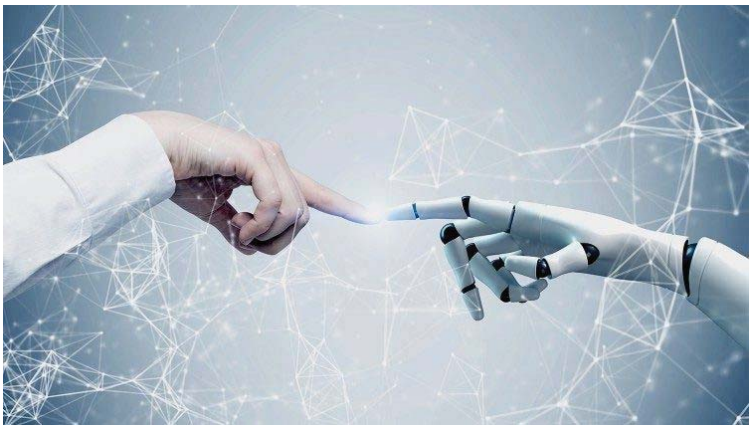
Tratto dal corso

"Didattica Digitale Integrata e Lavoro Agile – CYBERSECURITY & PRIVACY" – Luca Corbellini – 30/11/2020

CORBELLINI

Difenderci dai rischi

Per evitare il verificarsi di questo tipo di danni, occorre procedere parallelamente sia sotto il punto di vista tecnologico (adottando buone misure di «**Cyber Security**») sia sotto quello comportamentale (imparando le principali regole di «**igiene informatica**»).



Nelle prossime slide vedremo i principali pericoli e le misure per scongiurarli…

STUDIO TECNICO LEGALE CORBELLINI Studio AGLCOM. S.r.l

Difenderci dai rischi

Nel corso di questa esposizione troverà diverse volte citata la locuzione «**IGIENE INFORMATICA**»

Il significato potrebbe essere ignoto ai più, ma in realtà si tratta di quell'insieme di regole di comportamento rivolte all'**utente informatico** (non al tecnico esperto quindi), a cui si forniscono consigli volti ad aumentare il sua livello di sicurezza, promuovendo comportamenti dell'utente che migliorano la sua esperienza informatica sotto tutti gli aspetti.

Questa materia affronta temi legati alla privacy, alla riservatezza dell'utente, ai suoi diritti in rete, all'utilizzo «pieno» del web, saper trovare informazioni e farsi trovare; temi legati al rispetto degli altri utenti.

Fornisce piccoli e grandi consigli di autodifesa digitale per far faticare almeno un po' i criminali online interessati ai nostri dati ed alle nostre preferenze.

La materia è indipendente dalla piattaforma tecnologica che viene utilizzata (Spaggiari, Axios e Nuvola o registro elettronico o piattaforma didattica che sia) e sarà l'argomento di questa prima fase del corso.

Come dire… prima di usare l'autovettura, impariamo a riconoscere i segnali stradali !

STUDIO TECNICO LEGALE CORBELLINI Studio AGLCOM. S.r.l

il Ransomware

Che si tratti di falle del sistema tecnologico o che si tratti di nostra disattenzione, spesso i rischi derivano dal «download» (scaricamento sul proprio device durante la navigazione internet o mediante posta elettronica), di oggetti che funzionano come dei veri e propri «**cavalli di Troia**».

In questi anni una delle tecniche più utilizzate è quella del RANSOMWARE

ATTENZIONE !!!
QUESTI SONO DEI CRIMINALI, PAGARE IL RISCATTO NON DA' ALCUNA GARANZIA DI RIAVERE I PROPRI FILES

Il «RANSOMWARE» è un tipo di malware che, se lasciato entrare nel nostro device, si estende a tutti i file della rete (e non solo del singolo device) criptandoli e rendendoli del tutto inutilizzabili a noi fino al pagamento di un riscatto (di solito da pagare in bitcoin) per avere la chiave di decrittaggio e ripristinare la leggibilità di tutti i file.

Immaginate quanto grave possa essere il danno causato alla segreteria di una scuola da parte di un malware del genere, il server reso inutilizzabile, il backup altrettanto inutilizzabile se eseguito in locale su una unità connessa in rete in modo diretto…

STUDIO TECNICO LEGALE
CORBELLINI
Studio AGI.COM. S.r.l

il Phishing

Nel parlare comune è molto frequente assimilare un comportamento stupido a quello di un pesce, (Mario ha abboccato, Giuseppe è un boccalone etc.) e infatti, non a caso, questo malware è noto con il nome di PHISHING che in lingua inglese significa proprio «pesca».

Il guaio è che, in questo caso, i pesci che rischiano di abboccare

siamo noi !!!

Il «PHISHING» è una tecnica con cui un malintenzionato, tramite e-mail, banner, pop-up o altri sistemi trasmette degli «inviti» molto credibili che quasi sempre sembrano arrivare dalla nostra banca, da un nostro amico o da un nostro fornitore, che ci chiede di confermare dati personali, password, codici e altro ancora con l'intento subdolo di impossessarsene.

Questo sistema basa la sua efficacia sul furto di identità e sull'induzione all'errore che funziona tanto più sprovveduto è l'utente attaccato.

STUDIO TECNICO LEGALE
CORBELLINI
Studio AGI.COM. S.r.l

Difenderci dai rischi

Si è detto che per difendersi da questo tipo di rischi occorre adottare sia misure di sicurezza tecnologiche (software antivirus, firewall e connessioni internet sicure in primis), sia **comportamenti consapevoli**, vediamoli:

*Quando qualcuno ci contatta, via e-mail, con una finestra pop-up o in qualsiasi altro modo, prima di rispondere occorre verificare bene l'indirizzo del mittente, **assicurarsi che sia conosciuto**, che sia presente tra i nostri contatti, che il suo nome sia scritto correttamente, così come il testo del messaggio, **l'utilizzo di lingue straniere e la presenza di errori di ortografia è estremamente sospetta**…*

Gran parte delle e-mail di phishing provengono da indirizzi «strani», un caso tipico è quello di una e-mail con dominio **UNICREDITOBANCA** invece di **UNICREDITBANCA** dove la lettera «O» in più non viene notata da un utente che legge frettolosamente

Altre volte le mail provengono da indirizzi generici come

TIM@libero.it
BANCAINTESA@gmail.com

è molto improbabile che organizzazioni così grandi non abbiano un proprio dominio personale, di solito i loro indirizzi sono

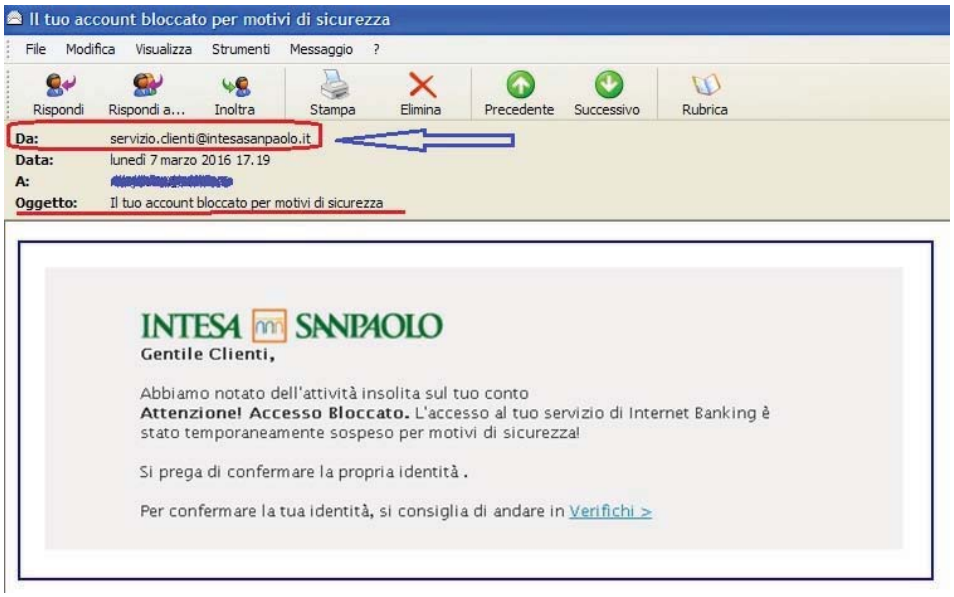
segnalazioneguasti@tim.it
mario.rossi@intesasanpaolo.com

Spesso queste mail sono **scritte in inglese** anche se dicono di provenire da istituzioni italianissime.

Altre volte contengono grossolani **errori di ortografia** e di battitura.

STUDIO TECNICO LEGALE CORBELLINI

Difenderci dai rischi



Ecco una tipica e-mail con cui malintenzionati chiedono ad un utente una fantomatica conferma dei dati di accesso al proprio conto corrente…

Nella realtà il sito della banca INTESA SAN PAOLO è un

.com

e non un

.it

STUDIO TECNICO LEGALE CORBELLINI

Difenderci dai rischi

LA MAIL-TRUFFA PER RUBARE I DATI PERSONALI

Da:* Presidenza Ingegneria <******@gmail.com>
Data:* 28 ottobre 2018 17:44:33 CET
A:* *******@**********
Oggetto:* *Referee request / Richiesta Referee - UniversitÃ *******

-[ENGLISH]---------

Dear *****,
we inform you that you have named as referee for a PhD course position, 11nd cycle, at the Università ***** (Italy).
We ask you kindly to fill in your reference letter by accessing our online service at the following link hXXp://*****.esse3.cineca.It with your credentials.
We also would like to inform you that the deadline for the reference letter submission is the: 5/11/2018 12:00:00 (italian time).

With our Best Regards
UNI**** staff
Online services of the Università Uni****

-[ITALIANO]---------

Gentile *****,
La informiamo che Lei è stato designato come referente a seguito della domanda di partecipazione al dottorato per il ciclo 11 presso l'Università *****.
Le chiediamo quindi di compilare la lettera di referenza accedendo al servizio on line attraverso il link hXXp://*****.esse3.cineca.It con le sue credenziali.

In questo caso ci sono due stranezze:

1) la mail proviene da un indirizzo generico (**gmail.com**), mentre l'università dispone certamente di un dominio personale.

2) Il link a cui rimanda è un indirizzo strano, privo di qualsiasi richiamo al nome dell'università

STUDIO TECNICO LEGALE CORBELLINI Studio AGLCOM. S.r.l

Difenderci dai rischi

[CASO : 850] **Il tuo account potrebbe essere oggetto di congelamento.**

Da: Staff di Libero **25 feb 2016** - 03:59

A:

LIBERO.

Siamo spiacenti di informarla che il suo account potrebbe essere oggetto di congelamento a causa di movimenti inusuali.

E forse uno dei seguenti motivi (Entra da un altro dispositivo, i tentativi di accesso errati, ecc.

Sblocca il tuo account

In assenza di conferma il tuo account sara congelatto.

© Libero 2016

Errori di battitura grossolani per una e-mail automatica proveniente da un importante provider.

1) Manca una parentesi ed inoltre l'italiano è «stentato»

2) Ci sono troppe «t» e manca l'accento sulla «a» di sarà

STUDIO TECNICO LEGALE CORBELLINI Studio AGLCOM. S.r.l

Difenderci dai rischi

TIM

Gentile cliente,

ABBIAMO notato Che hai pagato la bolletta Nello Stesso tempo Due volte.

Importo : 37 euro
Riferimento : TIM-A8005W

Per confermare il rimborso
Fare clic sul seguente link : http://rimborso.tim.it

Ti aspettiamo presto su www.tim.it.

Grazie da TIM.

MyTIM

Anche in questo caso non è credibile che un'azienda di prim'ordine come TIM scriva in modo così approssimativo

1) L'uso delle lettere maiuscole è isterico e anche la frase in italiano non è delle più fluenti.

2) Un'altra caratteristica è che, molto spesso, queste e-mail truffaldine, prospettano sconti, rimborsi o comunque vantaggi economici

STUDIO TECNICO LEGALE CORBELLINI Studio AGLCOM. S.r.l

Difenderci dai rischi

Altri comportamenti virtuosi che deve avere l'utente informatico:

*Oltre a verificare bene gli indirizzi di provenienza delle e-mail ed il modo in cui il testo è scritto, è bene diffidare da tutte quelle comunicazione che **inducono all'urgenza** al solo fine di determinare in chi le riceve uno stato di ansia e di fretta che impedisce l'approfondimento.*

*Inoltre queste e-mail sospette, **prospettano sempre vantaggi economici**, premi, rimborsi, sconti ed insperate eredità.*

STUDIO TECNICO LEGALE CORBELLINI Studio AGLCOM. S.r.l

Difenderci dai rischi

Inoltre:

*I siti internet seri che acquisiscono dati importanti (password, informazioni personali etc.) normalmente non utilizzano il normale protocollo **http://** ma la sua variante più sicura **https://**.*
La principale differenza consiste nel fatto che, nel secondo caso, la comunicazione tra il nostro device e il sito internet avviene in maniera protetta.

Negli esempi riportati alle slide precedenti (Unicredit, TIM, Banca Intesa etc.), possiamo stare certi che **nessuna di queste realtà utilizza siti basati su protocollo http:// ma tutti il più sicuro https://.**

Anche i siti che siamo abituati ad usare nel lavoro quotidiano (segreteria digitale, registro elettronico etc.) utilizzano il protocollo https://.

Per determinare la sicurezza o meno di un sito internet, i diversi browser utilizzano metodi diversi, di solito basati sull'icona raffigurante un lucchetto a fianco dell'indirizzo URL del sito

Quindi, se un sito ti chiede di inserire dati personali ed il suo URL non è anticipato dalla sigla https:// è bene sospettare che si tratti del sito sbagliato.

STUDIO TECNICO LEGALE CORBELLINI Studio AGLCOM. S.r.l

Difenderci dai rischi

Completiamo il discorso iniziato alla slide precedente suggerendo questa ulteriore cautela:

In una e-mail o su un sito, molto raramente i link recano l'intero indirizzo URL, è più frequente che il click venga richiesto su una icona, o su un testo come in questi esempi riportati a fianco

Se vuoi accedere alla tua area riservata clicca qui

Muovendoti con il cursore su queste icone o sui testi evidenziati, il puntatore cambia e si trasforma in una manina con l'indice puntato come questa

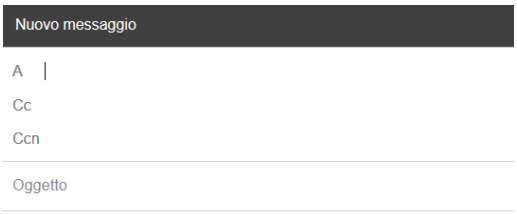
Contestualmente il browser, evidenzia l'intero URL a cui sarai indirizzato se farai il click, è questo il momento in cui verificare che l'indirizzo sia sicuro e che la pagina a cui si verrà indirizzati per l'inserimento dei dati sia di tipo **https://**.

STUDIO TECNICO LEGALE CORBELLINI Studio AGLCOM. S.r.l

Difenderci dai rischi

Prevenire i rischi è meglio che curare le ferite in un secondo tempo…

Quando mandi una e-mail a tanti destinatari, puoi scegliere di collocare i loro indirizzi su 3 barre denominate rispettivamente A… Cc… e Ccn…



Ricorda, se scriverai gli indirizzi nei campi A… e Cc… gli indirizzi saranno visibili a tutti (e quindi potresti violare la privacy di qualcuno), compresi quei malware che potrebbero essere presenti sui device dei destinatari e che saranno pronti ad impossessarsi di quegli indirizzi per farne un uso fraudolento…

STUDIO TECNICO LEGALE CORBELLINI Studio AGLCOM. S.r.l

Difenderci dai rischi

In conclusione di questa carrellata di semplici misure di igiene informatica da adottare per la sicurezza nostra e della nostra scuola, è giunto il momento di dedicare qualche slide a quella che, fin dalla nascita del primo Personal Computer, è la misura di sicurezza informatica per eccellenza.

la PASSWORD
(PAROLA CHIAVE)

Ciascuno di noi ne ha almeno una, tanti di noi ne hanno centinaia.

Alcune ci servono per ottenere degli sconti quando andiamo in profumeria o dal parrucchiere…

Altre, come il PIN del bancomat o quella del nostro home banking, sarebbero capaci di mandarci in rovina se le dovessimo perdere…

A scuola ci servono per registro elettronico, per l'utenza della segreteria digitale, per la posta, la piattaforma didattica e altro ancora !

STUDIO TECNICO LEGALE CORBELLINI Studio AGLCOM. S.r.l

Difenderci dai rischi

Per scegliere la tua password devi seguire la stessa logica che hai seguito per scegliere le chiavi che utilizzi normalmente nel mondo reale:

La tua bicicletta scassata

L'hai protetta con un lucchetto non proprio sicuro

Ma per la casa dove custodisci tutti tuoi averi e dove vivi con i tuoi cari

Hai preteso il meglio

Sii coerente anche con la password !

STUDIO TECNICO LEGALE
CORBELLINI

Difenderci dai rischi

Ricordati che per la legge le tue credenziali (nome utente e password) ti identificano legalmente.

Qualsiasi cosa venga fatta con la tua password, è come se l'avessi fatta tu.

Se la perdi o se è troppo facile da scoprire, qualcuno potrebbe usarla per qualcosa di illecito e poi incolpare te !

Difenderci dai rischi

Sono 3 i modi che utilizzano i malintenzionati per scoprire la tua password:

ATTACCO A DIZIONARIO

1

La forza di qualsiasi computer sta tutta nella velocità di elaborazione.
Per un hacker è un gioco da ragazzi creare un software che, in pochi secondi, faccia milioni di tentativi provando tutte le parole contenute nel dizionario.

Non usare parole troppo corte né comuni reali, inventane di tue…

Per esempio se vuoi che la tua password sia «attaccapanni» storpiala e fai in modo di scriverne una che non esista come ad esempio «atachpein»

Se userai lettere maiuscole e minuscole aumenterai la difficoltà, usa ad esempio «AtAchPein» e sarà ancora meglio se aggiungerai qualche **numero** come «1AtAchPein2»

Non fermarti, inserisci anche un **carattere speciale** come ad esempio «1AtAch#Pein2»

STUDIO TECNICO LEGALE
CORBELLINI
Studio AGLCOM. S.r.l

Difenderci dai rischi

FALSA RICHIESTA

2

Un sedicente tecnico che, di persona, tramite una telefonata o una e-mail, ti chiede di fornirgli la tua password affinché possa aggiornare il sistema o installare una nuova funzionalità

Da quando è entrato in vigore il G.D.P.R., tutti i software devono ispirarsi al principio di «**privacy by design**» ossia devono essere progettati fin dall'origine in modo da non violare le regole di riservatezza.

Questo significa che qualsiasi programma prevede che l'installazione degli aggiornamenti e tutta la manutenzione ordinaria possa essere eseguita tramite la password amministrativa del tecnico, senza chiedere quella personale dell'utilizzatore.

STUDIO TECNICO LEGALE
CORBELLINI
Studio AGLCOM. S.r.l

Difenderci dai rischi

INGENUITA' DELL'UTENTE

Abbiamo detto più volte come il primo nemico della nostra sicurezza informatica frequentemente siamo noi stessi.

3

Una password scritta su un post-it incollato sul monitor o sotto alla tastiera.

L'inserimento fatto senza assicurarsi che nessuno ci veda e che possa quindi capire quali tasti premiamo

STUDIO TECNICO LEGALE
CORBELLINI
Studio AGLCOM. S.r.l

Difenderci dai rischi

Una password robusta

Concludiamo ricordando che caratteristiche deve avere una password per essere definita «robusta» ed essere quindi resistente agli attacchi:

- Essere lunga almeno 8 caratteri
- Contenere sia caratteri maiuscoli che minuscoli
- Contenere numeri e caratteri speciali
- Non contenere riferimenti personali (nomi, date di nascita)
- Non derivare da nomi presenti in un normale dizionario
- Frequentemente cambiata (almeno ogni 3 mesi)
- Cambiata evitando piccole variazioni dalla precedente

Ricorda !
Quando abbandoni la tua postazione di lavoro (scrivania o cattedra che sia) devi disconnetterti oppure inserire uno screensaver protetto da password, altrimenti chiunque potrà accedere con la tua utenza.

STUDIO TECNICO LEGALE
CORBELLINI
Studio AGLCOM. S.r.l

Difenderci dai rischi

Il Back-up (copia di riserva)

In oltre 20 anni di assistenza tecnica informatica, non sono certo mancati gli **aneddoti** da raccontare; dagli interventi fatti a fronte di una semplice spina elettrica staccata dalla presa, ai ripristini software di computer di integerrimi signori ed elegantissime signore a causa di indicibili navigazioni su altrettanto impresentabili siti internet.

Solo un paio di volte però abbiamo visto clienti piangere dalla disperazione, in un caso uno studente venticinquenne per aver perso irrimediabilmente la copia della tesi di laurea che stava ultimando e nell'altro la Direttrice Amministrativa di un Istituto scolastico milanese per aver perso l'intero archivio di più anni contenuti nel gestionale SISSI.
Motivi molto diversi, nel primo caso la rottura fisica del disco fisso e nel secondo un virus, ma un denominatore comune: **in entrambi i casi non si erano premurati di eseguire il back-up periodico dei loro dati**.

STUDIO TECNICO LEGALE
CORBELLINI
Studio AGLCOM. S.r.l

Difenderci dai rischi

La regola è tanto semplice da risultare quasi disarmante, quanto più ritieni che siano importanti i tuoi dati, tanto meglio li devi proteggere da tutti quegli eventi che te li possono portare via e che, schematicamente, elenchiamo qui sotto:

Guasti tecnici	UN DISCO FISSO CHE SI ROMPE IRRIMEDIABILMENTE	IL RIPRISTINO DEI DATI DA UN DISCO ROTTO NON SOLO NON E' SEMPRE SCONTATO MA PUO' COMPORTARE UNA SPESA CONSIDEREVOLE
Malware	UN VIRUS CHE DISTRUGGE TUTTI I TUOI DATI	ANCHE IL MIGLIORE ANTIVIRUS TI PUO' TRADIRE, SORATTUTTO QUANDO IL VIRUS E' RECENTE E NON ANCORA ADEGUATAMENTE STUDIATO
Altri eventi	UN FURTO, UN INCENDIO, LO SMARRIMENTO DI UNA CHIAVETTA USB	POCO SI PUO' FARE CONTRO GLI IMPREVISTI, MA MOLTI DI QUESTI EVENTI NON SONO POI COSI' «IMPREVEDIBILI»

LA SOLUZIONE PIU' IMMEDIATA, ECONOMICA E SICURA E' UNA SOLA, **AVERE UNA COPIA DI BACK-UP DEI DATI**

Difenderci dai rischi

Un back-up efficace

Un back-up, per essere veramente efficace, deve avere queste caratteristiche:

Deve essere **completamente automatico**, se dipende da te sarà molto probabile che non lo farai perché te ne dimenticherai, o riterrai di non averne il tempo, se invece fosse automatizzato e partisse automaticamente durante la notte ad esempio, non solo sarai certo del fatto che andrà a buon fine, ma non ti disturberà durante il lavoro.

La copia dei dati deve essere **remota** ossia non collocata sullo stesso device, nella stessa stanza e se possibile nemmeno nella stessa casa, questo perché è ovvio che, se un ladro dovesse rubarti il PC, se la copia fosse contenuta in una chiavetta o un disco fisso esterno collegato stabilmente con il tuo device, con ogni probabilità ruberà anche tale periferica, inoltre i malware spesso danneggiano anche tutto ciò che è connesso e infine, volendo fare un esempio estremo ma non impossibile, un incendio che dovesse coinvolgere la tua scuola o la tua casa, rischierebbe di distruggere sia l'originale che la copia dei tuoi dati.

Deve essere **perfettamente protetto**, non dimenticare che nel mondo informatico la copia è esattamente identica all'originale, quindi le stesse precauzioni (password, antivirus etc.) che adotti per gli originali, devi adottarle anche per proteggere le tue copie.