UNIVERSITÀ DEGLI STUDI
DI MODENA E REGGIO EMILIA

Università degli Studi di Modena e Reggio Emilia

Via Università 4 - 41121- Modena (MO)
Tel: 059 2056511 - Fax: 059 245156
p.Iva 00427620364

Atto di Nomina dell'incaricato
Ai sensi e per gli effetti del D.Lgs. 30 Giugno 2003 n. 196

Università degli Studi di Modena e Reggio Emilia nella persona del suo Magnifico Rettore pro tempore in qualità di 'Titolare del Trattamento' dei dati personali, ai sensi e per gli effetti del art. 30 del D.Lgs 30 Giugno 2003 n. 196 con il presente atto NOMINA :

Lo studente Sig./Sig.ra .....
INCARICATO del trattamento dei dati personali.

Incaricato al trattamento dei dati personali.	
Acquisti	
Tipi di Dati : Dati Comuni	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • attività economiche, commerciali, finanziarie e assicurative
Vendite	
Tipi di Dati : Dati Comuni	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • attività economiche, commerciali, finanziarie e assicurative
Banca dati studenti ed ex studenti	
Tipi di Dati : Dati Comuni	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • dati relativi alla famiglia e a situazioni personali • istruzione e cultura • dati sul comportamento • Voti, giudizi e dati relativi al rendimento universitario
Tipi di Dati : Dati Sensibili	• origini razziali o etniche • convinzioni religiose • stato di salute • dati sensibili per portatori di Handicap
Posta elettronica	
Tipi di Dati : Dati Comuni	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • attività economiche, commerciali, finanziarie e assicurative • voti, giudizi ed altri dati di valutazione del rendimento scolastico
Ricerca	
Tipi di Dati : Dati Comuni	• nominativo, indirizzo o altri elementi di identificazione personale • dati relativi alla famiglia e a situazioni personali • dati sul comportamento • abitudini di vita o di consumo
Tipi di Dati : Dati Sensibili	• origini razziali o etniche • stato di salute
Personale universitario	
Tipi di Dati : Dati Comuni	• codice fiscale ed altri numeri di identificazione personale • nominativo, indirizzo o altri elementi di identificazione personale • dati relativi alla famiglia e a situazioni personali • dati relativi al tipo di lavoro ed alla retribuzione • istruzione e cultura • abitudini di vita o di consumo
Tipi di Dati : Dati Sensibili	• origini razziali o etniche • opinioni politiche • adesione a partiti • adesione a sindacati • stato di salute

	• dati sensibili per portatori di Handicap

Occorre prestare attenzione alle istruzioni per l'incaricato (Allegato 1) alle quali vi è l'obbligo di attenersi scrupolosamente.
Il presente incarico è collegato alle mansioni svolte da ciascun incaricato e necessario per lo svolgimento delle stesse, pertanto, non costituisce conferimento di nuova mansione o ruolo.
L'incaricato dichiara di aver ricevuto, in Allegato 1, le istruzioni e si impegna, dopo averne presa visione, ad adottare le misure necessarie alla loro attuazione.
In caso di violazione delle istruzioni impartite, gli Incaricati così nominati saranno responsabili per le conseguenze giuridiche che deriveranno, direttamente o indirettamente, dalla loro condotta attiva o omissiva a titolo di dolo o colpa.
Si rammenta che qualora nell'espletamento dell'incarico conferito si dovesse, anche accidentalmente o attraverso i colleghi avere notizia o venire a conoscenza di dati, documenti, informazioni o notizie riguardanti l'organizzazione, l'attività e/o il know-how specifico dell' Università, questi - fatte salve le notizie o le informazioni che siano o divengano di dominio pubblico - sono di esclusiva proprietà dell' Università e a carattere assolutamente riservato.
Pertanto, sia nel corso dell'espletamento dell'attività lavorativa che dopo, è necessario mantenere il più rigoroso riserbo sulle suddette informazioni, notizie e dati, non divulgarli o renderli in alcun modo disponibili a terzi , né utilizzarli per scopi diversi dai servizi che si eseguono per conto dell'Università.
E' vietato conservare, commercializzare, divulgare, trasmettere a terzi in qualsivoglia forma i dati dell'Università se non per svolgere attività istituzionale. Le modalità di raccolta e di comunicazione sono specificate nell'allegato 1.

La firma del presente incarico costituisce consapevole accettazione degli obblighi assunti.

Per accettazione
FIRMA

.....

Modena/Reggio Emilia .....

VISTO
DELL STRUTTURA

_____

UNIVERSITÀ DEGLI STUDI
DI MODENA E REGGIO EMILIA

Università degli Studi di Modena e Reggio Emilia

Via Università 4 - 41121 - Modena (MO)
Tel: 059 2056511 - Fax: 059 245156
P.Iva 00427620364

Allegato 1

Istruzioni per l'incaricato

La legge definisce come incaricati "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile".

Limitatamente all'ambito di competenza a lei assegnato nella Nomina dal Titolare o dal Responsabile, vengono sotto riportate le istruzioni a cui è tenuto ad attenersi nel trattamento di dati personali, in conformità alle normative vigenti sulla Privacy.

PROCEDURE PER LA CLASSIFICAZIONE DEI DATI.

L'incaricato deve essere sempre in grado di individuare il tipo di dato che sta trattando secondo quanto stabilito dalla Legge.

La natura dei dati trattati

La Legge definisce "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Vengono riportate di seguito le definizioni :

• dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato;

• dati sensibili: la lettera d) del comma 1 dell'articolo 4 del codice definisce in tale modo i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

• dati giudiziari: tali sono considerati, dalla lettera e) del comma 1 dell'articolo 4 del codice, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u) del Dpr 313/2002, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

• dati che presentano rischi specifici: sono quelli previsti dall'articolo 17. Si tratta di dati che, pur non essendo sensibili o giudiziari, presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato in relazione alla natura dei dati, ovvero alle modalità di trattamento o agli effetti che esso può determinare.

In considerazione di tale fatto, il loro trattamento è ammesso nel rispetto delle misure e degli accorgimenti, ove previsti, prescritti dal Garante a garanzia dei soggetti interessati.

AFFIDAMENTO AGLI INCARICATI DI DOCUMENTI, CONTENENTI DATI PERSONALI, E MODALITA' DA OSSERVARE PER LA CUSTODIA DEGLI STESSI.

TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Per il trattamento dei documenti cartacei rispettare sempre le indicazioni del Titolare o del Responsabile in merito agli archivi a cui poter accedere e ai documenti che è possibile trattare: non trattare nessun documento al di fuori delle autorizzazioni.

Una volta presi in carico, gli atti e i documenti, contenenti dati personali, non devono essere lasciati liberi di vagare senza controllo ed a tempo indefinito per gli uffici, ma occorre provvedere in qualche modo a controllarli e custodirli, per poi restituirli al termine delle operazioni affidate.

In caso di affidamento di atti e documenti contenenti dati sensibili o giudiziari, il controllo e la custodia devono avvenire in modo tale che ai dati non accedano persone prive di autorizzazione. A tale fine è quindi necessario dotarsi di cassetti con serratura o di altri accorgimenti aventi funzione equivalente, nei quali

riporre i documenti contenenti dati sensibili o giudiziari prima di assentarsi dal posto di lavoro, anche temporaneamente (ad esempio, per recarsi in mensa oppure alla macchinetta del caffè).

Assicurare l'accesso a tali archivi alle sole persone autorizzate ricordando loro di non abbandonare mai tali documenti e di riconsegnarli non appena terminato l'incarico che ne ha determinato il trattamento.

Qualora si debbano utilizzare anche nei giorni successivi i documenti potranno essere riposti in tali cassetti al termine della giornata di lavoro. Al termine del trattamento dovranno invece essere restituiti all'archivio.

Si ricorda inoltre che i certificati medici contengono dati sensibili ai fini privacy pertanto devono essere consegnati in busta chiusa al proprio Responsabile che provvederà a farlo recapitare all'ufficio personale. Nei luoghi provvisti di cassetta della posta predisposta per i certificati medici si prega di volerli inserirli all'interno.

Qualora si richiedano le chiavi degli uffici e/o degli armadi che normalmente vengono chiusi a chiave si ricorda che chi richiede le chiavi è direttamente responsabile e che le chiavi non devono essere lasciate libere di vagare senza controllo ed a tempo indefinito, ma occorre provvedere in qualche modo a controllarle e custodirle, per poi restituirle al termine delle operazioni affidate alla persona a cui sono state richieste.

Si rammenta inoltre che in Università è consentito il riutilizzo della carta per contenere i costi e per rispettare l'ambiente. Si chiede però ad ogni incaricato di riutilizzare carta che non contenga dati di tipo personale e/o sensibili.

MODALITA' PER ELABORARE E CUSTODIRE LE PASSWORD, NONCHE' PER FORNIRNE UNA COPIA AL PREPOSTO ALLA CUSTODIA DELLE PAROLE CHIAVE.

TRATTAMENTO CON L'AUSILIO DI STRUMENTI ELETTRONICI

Si ricorda che l'utilizzo degli strumenti informatici deve essere effettuato rispettando la normativa vigente. Utilizzare sempre le credenziali di autenticazione (user ID e Password) fornite dall'Amministratore di Sistema o dal Responsabile dell'area sicurezza. Mai utilizzare il pc senza avere le credenziali di autentificazione. Qualora il pc ne fosse sprovvisto l'incaricato stesso dovrà comunicarlo al proprio Responsabile che dovrà provvedere all'attivazione.

Le credenziali di autenticazione sono assolutamente personali e non cedibili, per nessuna ragione.

Se si è in possesso di più credenziali di autenticazione, fare attenzione ad accedere ai dati unicamente con la credenziale relativa al trattamento in oggetto.

Elaborare le password seguendo le istruzioni sotto riportate (vedi sotto)

Su ogni singola unità (Pc) non devono risiedere dati di alcun genere. Tutti i dati devono essere salvati in rete dove verranno adottate tutte le misure minime richieste dall'all. B del D.Lgs 196/2003 .

I SISTEMI INFORMATICI UNIVERSITARI

Il personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati all'incaricato sono, come è noto, strumenti di lavoro, pertanto: tali strumenti vanno custoditi in modo appropriato e possono essere utilizzati solo per fini professionali e non per scopi personali, tanto meno per scopi illeciti; debbono essere prontamente segnalati all'Università il furto, danneggiamento o smarrimento di tali strumenti.

Poiché in caso di violazioni contrattuali e giuridiche, sia l'Università, sia il singolo incaricato sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Università verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole, l'integrità del proprio sistema informatico e la coerenza delle sue configurazioni e dei suoi archivi con le finalità universitarie .

In questo contesto l'Università potrà per necessità di sicurezza universitaria o per esigenze di continuità della normale attività lavorativa, accedere agli archivi di corrispondenza elettronica o ai file di log riservati alla tracciatura degli eventi di connessione.

Utilizzo del personal computer

• é consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal Titolare o dal Responsabile; non è consentito scaricare file dalla rete o contenuti in supporti magnetici e/o ottici non aventi alcuna attinenza con la propria prestazione lavorativa;
• non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
• non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come ad esempio i modem);
• non è consentito condividere file, cartelle, hard disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati di peer to peer al fine di scaricare materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.);
• i Personal Computer "stand alone" o in rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività universitaria non può essere dislocato, nemmeno per brevi periodi, in queste unità; l'Università si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione delle presenti istruzioni.

Utilizzo di internet

• non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni ;
• a maggior ragione non è consentito navigare in siti che accolgono contenuti contrari alla morale e alle prescrizioni di Legge se non per fini di ricerca universitaria;
• non è inoltre consentito navigare in siti che possano rivelare una profilazione dell'individuo definita 'sensibile' ai sensi del D.Lgs. 196/2003: quindi siti la cui navigazione palesi elementi attinenti alla fede religiosa, alle opinioni politiche e sindacali del dipendente o le sue abitudini sessuali;
• non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal Titolare o dal Responsabile del Trattamento e con il rispetto delle normali procedure di acquisto;
• non è consentito lo scarico di software gratuiti trial, freeware e shareware prelevati da siti Internet, se non espressamente autorizzato dal Titolare o dal Responsabile;
• non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) né attraverso Internet né attraverso servizi di peer to peer;
• è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività universitaria;
• non è permessa la partecipazione, per motivi non legati all'attività universitaria a Forum e giochi in rete pubblica, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);
• non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Utilizzo del servizio di posta elettronica

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:
• non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle proprie mansioni;
• non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
• la posta elettronica diretta all'esterno della rete informatica universitaria può essere intercettata da estranei, e dunque, non deve essere usata per inviare informazioni, dati o documenti di lavoro "strettamente Riservati";
• non è consentito l'utilizzo dell'indirizzo di posta elettronica universitaria per la partecipazione a dibattiti, Forum o mail-list; solo in questo ultimo caso è possibile, previa autorizzazione per la verifica della validità dell'emittente, iscriversi a servizi di informazione strettamente inerenti all'attività universitaria;
• poichè esiste un dominio di proprietà universitaria (es.: unimore.it) al quale è collegato un servizio di posta e la relativa casella (es.: mario.rossi@unimore.it), non è consentito utilizzare web mail esterni, ovvero caselle di posta elettronica non appartenenti al dominio o ai dominii universitari salvo diversa ed esplicita autorizzazione.

MODALITÀ PER ELABORARE E CUSTODIRE LE PASSWORD

Le credenziali di autenticazione sono assolutamente personali e non cedibili, per nessuna ragione.

Se si è in possesso di più credenziali di autenticazione, fare attenzione ad accedere ai dati unicamente con la credenziale relativa al trattamento in oggetto.

Elaborare le password seguendo le istruzioni sotto riportate.

SCELTA DELLE PASSWORD

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

COSA NON FARE

• NON dire a nessuno la propria password. Lo scopo principale per cui si usa una password è assicurare che nessun altro possa utilizzare le risorse altrui o possa farlo a nome altrui.
• NON scrivere la password in un posto accessibile, soprattutto vicino al computer.
• Quando si immette la password NON mostrare ad altri quello che sta battendo sulla tastiera.
• NON scegliere password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.
• usare parole straniere NON renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
• NON usare il proprio nome utente. È la password più semplice da indovinare.
• NON usare password che possano in qualche modo essere legati a situazioni personali, ad esempio, il proprio nome, quello del coniuge, dei figli, del cane, date di nascita, numeri di telefono etc.

COSA FARE OBBLIGATORIAMENTE

• la password deve essere composta da almeno otto caratteri o, se il sistema non l'accetta, da un numero di caratteri pari a quello consentito dal sistema; è buona norma che, di questi caratteri, da un quarto alla metà siano di natura numerica;
• l'incaricato deve provvedere a modificare la password immediatamente, non appena la riceve per la prima volta, da chi amministra il sistema;
• la password deve essere modificata dall'incaricato almeno ogni 6 mesi;
• se il trattamento riguarda dati sensibili o giudiziari la password deve essere modificata almeno ogni tre mesi ;
• coloro che gestiscono in modo autonomo i pc dell'Università devono provvedere da sè alla modifica della password.

COSA FARE PRATICAMENTE

Utilizzare più di una parola e creare password lunghe

A volte è più semplice ricordare una frase completa di senso compiuto piuttosto che una parola complicata. Questa tecnica oltre a facilitare la memorizzazione migliora la sicurezza della parola chiave: la lunghezza influisce sulle difficoltà di individuazione e consente di utilizzare lo "spazio" tra una parola e l'altra come ulteriore elemento da intercettare.
Inoltre è bene sapere che diversi strumenti di intercettazione presumono che le password non siano formate da più di 14 caratteri quindi, anche senza complessità, le password molto lunghe (da 14 a 128 caratteri) possono rappresentare un ottima protezione contro possibili violazioni. Non tutti i software sono tuttavia in grado di accettare password superiori a 14 caratteri: ad esempio i sistemi operativi Windows 95 98 e Mc non oltrepassano questo limite.

Utilizzare numeri e simboli al posto di caratteri

Non limitarsi alle sole lettere ma, dove possibile, utilizzare l'ampia gamma di minuscole/maiuscole, numeri e simboli a disposizione sulla propria tastiera:
• Caratteri minuscoli: a, b, c,...
• Caratteri maiuscoli: A, B, C,...
• Caratteri numerici: 0,1,2,3,4,5,6,7,8,9
• Caratteri non alfanumerici: (< > , .) ` ~ ! $ % ^ ; * - + = | \ { @ # } [/] : ; " '?

Non inserirli alla fine di una parola nota come ad es.:"computer987". In questo caso la password può essere identificata abbastanza facilmente: la parola "computer" è inclusa in molti dizionari contenenti nomi comuni e quindi dopo aver scoperto il nome restano solo 3 caratteri da identificare. Al contrario, è sufficiente sostituire una o più lettere all'interno della parola con simboli che possono essere ricordati facilmente. Ad esempio si può provare a utilizzare "@"al posto di "A", "$"al posto di "S", zero (0) o la doppia parentesi () al posto di "O", e "3"al posto di "E": si tratta di trovare delle analogie che ci rendano familiare la sostituzione di lettere con simboli e numeri. Con alcune sostituzioni si possono creare password riconoscibili per l'utente, ad esempio (es.: "Ve$tit0 di Mari0"), già sufficientemente lunghe e estremamente difficili da identificare o decifrare.

Cercare di realizzare password utilizzando caratteri appartenenti a tutti i quattro gruppi rappresentati nella lista.

OBBLIGO DI NON LASCIARE INCUSTODITI E ACCESSIBILI GLI STRUMENTI ELETTRONICI, MENTRE È IN CORSO UNA SESSIONE DI LAVORO.

Non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. È necessario terminare la sessione di lavoro, al computer, ogni volta che ci si deve allontanare, anche solo per cinque minuti effettuando un log out o mettendo in atto accorgimenti tali, per cui anche in quei cinque minuti il computer non resti:

• incustodito: può essere sufficiente che un collega rimanga nella stanza, durante l'assenza di chi sta lavorando con lo strumento elettronico, anche se la stanza rimane aperta;
• accessibile: può essere sufficiente chiudere a chiave la stanza, dove è situato lo strumento elettronico, durante l'assenza, anche se nella stessa non rimane nessuno.

Non si devono invece mai verificare situazioni in cui lo strumento elettronico venga lasciato attivo, durante una sessione di trattamento, senza che sia controllato da un incaricato al trattamento o senza che la stanza in cui è ubicato venga chiusa a chiave.
E' possibile installare strumenti software specifici (es.: screen saver) che, trascorso un breve periodo di tempo predeterminato dall'utente in cui l'elaboratore resta inutilizzato, non consentono l'accesso all'elaboratore se non digitando una password.

PROCEDURE E MODALITÀ DI UTILIZZO DEGLI STRUMENTI E DEI PROGRAMMI ATTI A PROTEGGERE I SISTEMI INFORMATIVI.

• Aggiornare con cadenza almeno mensile gli antivirus installati sulla propria postazione PC. Si consigliano ovviamente cadenza più serrate.
• Installare le Patch di aggiornamento dei sistemi operativi e dei programmi utilizzati per il trattamento dati personali, con cadenza annuale che diviene semestrale in caso di trattamenti di dai sensibili o giudiziari.

FATTORI DI INCREMENTO DEL RISCHIO E COMPORTAMENTI DA EVITARE

• riutilizzo di Cd/dvd/Chiavette Usb i già adoperati in precedenza;
• uso di software gratuito (trial, freeware o shareware) prelevato da siti Internet o in allegato a riviste o libri;
• collegamento in Internet con download di file eseguibili o documenti di testo da siti web o da siti FTP;
• collegamento in Internet e attivazione degli applets di Java o altri contenuti attivi;
• file attached di posta elettronica.

LINEE GUIDA PER LA PREVENZIONE DEI VIRUS

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Come prevenire i virus:

1. Usare soltanto programmi provenienti da fonti fidate
Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzare programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

2. Assicurarsi che il proprio software antivirus sia aggiornato
La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Informarsi attraverso il Portale della privacy sugli obblighi di legge in tema di aggiornamento degli antivirus e applicare, se possibile, una frequenza di aggiornamento mensile (più idonea di quella prevista dalla legge).

3. Assicurarsi che il proprio PC sia stato controllato dall'antivirus
Almeno una volta alla settimana lanciare una scansione dell'intero sistema con il software antivirus. Se questo software lo prevede, schedulare anche in questo caso la programmazione della scansione in maniera tale da non doversi ricordare di lanciarla e lasciando che il programma la esegua in automatico. Consultarsi con il proprio Responsabile o con il Titolare per le informazioni necessarie.

4. Non diffondere messaggi di provenienza dubbia
Si devono ignorare i messaggi che avvisano di un nuovo virus pericolosissimo: le mail di questo tipo sono dette con terminologia anglosassone hoax (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete.
Questo anche se il messaggio sembra provenire dal proprio responsabile, da un collega o da un tecnico informatico. Da ricordare che spesso sembra essere "una notizia proveniente dalla Microsoft" oppure dall'IBM (sono gli hoax più diffusi).

5. Non partecipare a "catene di S. Antonio" o simili
Analogamente, tutti i messaggi che invitano a "diffondere la notizia quanto più possibile" sono hoax. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti hoax aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso.

6. Evitare la trasmissione di file eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computer in rete

7. Non utilizzare i server di rete come stazioni di lavoro

8. Non aggiungere dati o file Cd, Dvd o chiavette Usb contenenti programmi originali

9. Non far partire accidentalmente il computer da Cd o Dvd o chiavetta Usb
Infatti se il Cd, Dvd o la chiavetta Usb fossero infettati, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri files.

10. Proteggere i Cd e/o DVD da scrittura quando possibile.
In questo modo si evitano le scritture accidentali, magari tentate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.
• Non utilizzare il proprio Cd e/o Dvd di sistema su un altro computer se non in condizioni di protezione in scrittura;
• Se si utilizza un computer che necessita di essere avviato da Cd e/o Dvd, usare un Cd e/o un Dvd protetto in scrittura;
• Non attivare mai da Cd e/o Dvd un sistema basato su hard disk a meno di utilizzare un disco di sistema, protetto in scrittura e sicuramente non infetto.

OBBLIGO DI RISERVATEZZA E CAUTELA NELLA COMUNICAZIONE A TERZI DI DATI E INFORMAZIONI

Anche informazioni di normale quotidianità universitaria o ritenute non riservate all'interno dell'interscambio tra incaricati, assumono diversa importanza, e quindi necessitano di una maggiore tutela, se comunicate all'esterno a soggetti terzi. La salvaguardia delle informazioni e dei dati oltre ad essere un requisito fondamentale per la sicurezza del patrimonio informativo universitario, è anche un espresso obbligo di legge nei confronti di qualsiasi soggetto definito "interessato". A fronte di tali motivazioni è importante ribadire la necessità di osservare ogni cautela nel trasferire all'esterno qualsiasi informazione proporzionalmente al loro contenuto e all'attendibilità dell'interlocutore.

SOCIAL ENGINEERING

Il social engineering è l'insieme delle tecniche psicologiche usate da chi vuole indurre ai propri scopi presentandosi personalmente o con un contatto dall'esterno a mezzo telefono o posta elettronica. Gli obiettivi possono andare dalla raccolta di informazioni apparentemente innocue riguardanti l'Università o la sua organizzazione e il personale che vi lavora e possono arrivare a toccare dati riservati.
Con l'ausilio di messaggi studiati o abili tecniche di persuasione l'aggressore può rendere l'interlocutore complice inconsapevole di azioni che andranno a suo beneficio come, ad esempio, l'acquisizione di informazioni o l'ottenimento della fiducia del personale, l'apertura di allegati infetti o la visita di un sito che contiene dialer o altro materiale pericoloso. Rispetto al social engineering via e-mail, uno dei principali problemi degli autori di virus è che molti utenti utilizzano strumenti di difesa aggiornati che non consentono l'esecuzione in automatico di applicativi e quindi non consentono l'attivazione di programmi dannosi. Per scavalcare queste precauzioni e quindi lanciare il virus, c'è un modo molto semplice: indurre la vittima, tramite espedienti psicologici a fidarsi dell'allegato e quindi eseguirlo, o fidarsi del collegamento ad un sito web contenuto nel messaggio e quindi raggiungerlo.
In questo senso l'aggressore potrebbe essere capace di sfruttare i punti di debolezza redigendo abili messaggi che, inducendo fiducia o curiosità, riescono ad arrivare allo scopo.

E-MAIL PHISHING

Un altro scopo degli aggressori è indurre l'utente a fidarsi dell'intero contenuto di un messaggio di posta elettronica e quindi ottenere una fedele esecuzione delle istruzioni contenute: ad esempio, vengono inviate false comunicazioni e-mail aventi grafica, forma, autorevolezza e loghi ufficiali di enti noti, banche, intermediari finanziari, assicurazioni, etc., chiedendo informazioni attraverso moduli o link a pagine web debitamente camuffate. In questa modo vengono richieste, ad esempio, password, numeri di carta di credito o altre informazioni riservate senza che in realtà la raccolta dati abbia nulla a che vedere con l'organismo ufficiale imitato. La vittima crede di comunicare con essi ma in realtà sta trasmettendo informazioni riservate all'aggressore.
Spesso queste tecniche sono abbinate tra loro e utilizzate più volte nel tempo nei confronti della stessa vittima.

COSA FARE

• non fornire informazioni confidenziali al telefono o di persona a interlocutori non conosciuti;
• limitarsi a fornire informazioni a interlocutori noti e con i quali si opera per disposizioni universitarie, nei limiti dei contenuti afferenti al proprio ambito lavorativo;
• diffidare dei messaggi provenienti da fonte non conosciuta;
• non aprire messaggi provenienti da fonte non conosciuta contenenti allegati;
• non aprire messaggi contenenti allegati sospetti;
• non utilizzare link contenuti nel testo del messaggio perché possono essere facilmente falsificati; in questi casi si deve andare direttamente sul sito citato digitandone da capo il nome;
• non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonte sconosciuta;
• non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonti istituzionali o apparentemente conosciute (ad es.: banche) in quanto tali strutture non richiedono mai dati utilizzando questa modalità;
• in caso di dubbio è sempre preferibile verificare l'attendibilità delle richieste con il Responsabile o il Titolare.

CUSTODIA ED UTILIZZO DEI SUPPORTI RIMOVIBILI, CONTENENTI DATI PERSONALI.

Particolare attenzione deve essere dedicata ai supporti rimovibili (es. Cd, Dvd, chiavette Usb), contenenti dati sensibili o giudiziari, nei seguenti termini:
• i supporti rimovibili (es. Cd, Dvd, chiavette Usb), contenenti dati sensibili o giudiziari devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti:. E' bene adottare archiviazioni in modo che vengano conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi.
• Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.
I supporti removibili (es. Cd, Dvd e chiavette Usb) che contengono dati sensibili e/o giudiziari dovranno essere di tipo criptato .