Indicazioni di base in materia di sicurezza dei dispositivi utilizzati - 10 punti essenziali –

Versione 1.0

Sommario

Premessa

Forniamo agli studenti e al personale strutturato di Ateneo **alcune indicazioni di base utili a preservare la sicurezza cibernetica dei dispositivi** personali o messi a disposizione dalle strutture universitarie **al fine di evitare o di ridurre l'impatto delle possibili conseguenze di furti, usi non appropriati o non autorizzati di dati e/o credenziali personali utilizzabili** nell'ambito dei servizi offerti dall'università.

1. Effettua gli aggiornamenti di sistemi operativi, anti-malware e software installati

Per proteggere il tuo pc od il tuo telefono cellulare dalle minacce alla sua sicurezza **è essenziale che aggiorni periodicamente il suo sistema operativo, l'antivirus e i software in esso installati**.

Visita il sito web ufficiale dell'azienda produttrice del sistema operativo installato sul tuo dispositivo per ricevere ulteriori informazioni in merito alla configurazione degli aggiornamenti.

2. Usa un anti-malware di tipo professionale

I software anti-malware rappresentano una difesa efficace contro le minacce alla vulnerabilità del dispositivo fisso o mobile.

Per tutti i suoi dipendenti e per personale strutturato l'Università degli Studi di Milano mette a disposizione per il download un software anti-malware utilizzabile anche sui dispositivi personali. Per ottenere informazioni più dettagliate in merito **visita la sezione "Servizio antivirus" della intranet** (è necessaria l'autenticazione per effettuare il download gratuito dell'antivirus).

Se non sei un dipendente o un collaboratore dell'Ateneo, ti suggeriamo di installare un software anti-malware professionale con licenza d'uso personale: così facendo, garantirai al tuo dispositivo un livello di sicurezza maggiore rispetto a quella offerta dai programmi forniti con i più recenti sistemi operativi o dai software di tipo freeware.

3. Effettua backup periodici

Il backup è l'unico sistema certo per recuperare dati anche a fronte di danni subiti dall'hard disk e/o dovuti all'azione di malware: non esistono, infatti, software che offrono garanzie di protezione assoluta. Per comprendere cosa fare, consulta le guide disponibili on line sui siti web ufficiali dell'azienda che ha prodotto il tuo dispositivo, quello ufficiale dell'organizzazione che ha realizzato il sistema operativo in esso installato o quelle messe a disposizione sulla intranet di Ateneo.

4. Cambia le tue password con regolarità e scegline di difficili o usa l'autenticazione a più fattori

Ricordati di modificare con frequenza (almeno una volta ogni tre-sei mesi) le tue password onde prevenire il rischio di un loro utilizzo da parte di malintenzionati, seguendo le indicazioni reperibili su http://www.unimi.it/studenti/61957.htm o https://work.unimi.it/servizi/servizi_tec/59030.htm .

Ti raccomandiamo di **non utilizzare un servizio di generazione di password fornito via web**, **dato che queste ultime potrebbero essere intercettate** mentre le invii ed utilizzate successivamente a scopi malevoli.

5. Verifica se il tuo username è collegato ad incidenti informatici

Può essere utile **verificare periodicamente che il proprio username (ad es. account di posta elettronica) non compaia nelle basi di dati legate a servizi web sottratte da criminali informatici e messi a disposizione on-line nel così detto "deep web"(risorse web non indicizzate dai motori di ricerca).**

Un servizio molto utile in tal senso è fornito dal sito webhttps://www.haveibeenpwned.com il quale, dopo aver effettuato un confronto tra gli archivi degli account compromessi e gli indirizzi email degli utenti che ad esso si iscrivono, invia tempestivamente a questi ultimi una notifica allo scopo di avvisarli di un rischio potenziale per la loro privacy e la loro sicurezza.

Attenzione, la presenza dello username associato al dominio di unimi.it non vuol dire che sono state violate le credenziali di Ateneo! Potrebbe ad esempio essere connesso a violazione di siti o servizi esterni per i quali sia stato usato come codice identificativo l'indirizzo di posta dell'Università.

6. Elimina gli account di posta elettronica che non utilizzi e disiscriviti dai servizi web che non ti servono

Ricordati di eliminare gli account di posta elettronica che hai creato nel corso del tempo e di disiscriverti dai servizi web che non utilizzi più: tanto più è grande il numero di account che hai creato e/o di servizi erogati via web a cui ti sei iscritto, quanto più ti esponi al rischio, minimizzabile, che le tue credenziali o i tuoi dati personali vengano sottratti.

7.Naviga in rete in sicurezza, ma presta attenzione ad alcuni dei plugin per browser utilizzabili

Utilizza web browser noti e aggiornarli costantemente (operazione che teoricamente effettuata in automatico da quelli principalmente usati).

Ricordati, inoltre, che installando apposite estensioni per browser (o plug-in) puoi proteggere ulteriormente la tua privacy e la sicurezza del tuo dispositivo mentre navighi su internet. Estensioni che blocchino annunci, ad esempio, possono aiutarti ad impedire che i disclaimer dannosi infettino il tuo computer con malware o possono informarti sull'affidabilità di un sito web.

Attenzione, però! Alcuni plugin per browser di cui potresti servirti per incrementare il livello di sicurezza della navigazione web potrebbero infettare il tuo pc! Informati bene prima di procedere con **la loro installazione** se non sei sicuro della loro origine.

8. Presta attenzione ai tuoi dispositivi mobili e annota il loro codice IMEI

La perdita o la sottrazione del tuo dispositivo mobile (cellulare, laptop o tablet) è un rischio concreto in cui tutti possono incappare.

E' teoricamente possibile rintracciare il tuo dispositivo in modi diversi: attraverso un servizio appositamente creato dalla sua casa produttrice, tramite apposite app o analizzando la cronologia degli spostamenti eseguiti / in esecuzione mentre si è loggati ad un account di posta elettronica / social network.

A titolo precauzionale, in ogni caso, **annota sempre da qualche parte il codice IMEI** del tuo dispositivo prima di servirtene (verificane la presenza sulla scatola / retro del dispositivo / vano batteria): **in caso di furto o perdita di un cellulare, ad esempio, ti servirà per impedirne l'uso da parte di estranei e di rintracciarlo.**

9. Usa la crittografia

Sempre più dispositivi e sistemi operativi rendono la crittografia disponibile, a basso impatto e facile da configurare. **Utilizzando la crittografia, ove possibile, si protegge la privacy e la riservatezza dei dat**i. Visita il sito web ufficiale dell'aziende che ha prodotto il dispositivo che utilizzi per ricevere ulteriori informazioni utili o consulta le linee guida di Ateneo per approfondire il tema.

10. Vigila sulla tua privacy e la tua sicurezza

Leggi le nostre linee guida in materia di Privacy e security o consulta gli avvisi di sicurezza pubblicati periodicamente sulla intranet di Ateneo: troverai suggerimenti utili ed indicazioni sempre aggiornate.