UNIVERSITÀ DEL SALENTO

Raccomandazioni in tema di cyber security nell'uso degli strumenti informatici di lavoro

a cura della Ripartizione Tecnica e Tecnologica – Area Gestione Infrastrutture

Ultimo aggiornamento: novembre 2018

SOMMARIO

1. SCOPO DEL DOCUMENTO

Le minacce cibernetiche sono oggi innumerevoli e, oltre a sfruttare le vulnerabilità dei sistemi informatici, fanno spesso leva sulla scarsa consapevolezza dei rischi da parte degli utenti e quindi su loro comportamenti non sempre adeguati a causa di conoscenze limitate o perché indotti da tecniche di "ingegneria sociale".
Tali minacce mettono a rischio la sicurezza dei dati trattati e la disponibilità degli strumenti di lavoro.
Lo scopo di questo documento è di fornire agli utenti raccomandazioni e informazioni utili ad un uso consapevole degli strumenti informatici di lavoro intesi sia come servizi (es. posta elettronica, web, ecc.) che come dispositivi (pc desktop, laptop, tablet, smartphone, ecc..) riguardo agli aspetti legati alla sicurezza. Consapevolezza, una buona dose di attenzione e alcune corrette abitudini sono uno strumento molto potente di difesa contro tali minacce.

2. COLLEGAMENTO ALLA RETE

Per ragioni di sicurezza e di prestazioni, ove possibile è sempre consigliato collegare i dispositivi informatici di lavoro alla rete d'Ateneo tramite connessione cablata.
Qualora si dovesse utilizzare la connessione Wi-Fi, il SSID "Eduroam" è da preferire a quello "Unisalento".
Qualora vi fosse la necessità di collegare un dispositivo mobile a reti Wi-Fi gestite da soggetti terzi, assicurarsi di utilizzare solo reti wireless protette da password, con protocollo almeno WPA2 e di proprietà di enti accreditati (è bene verificarne la reale proprietà con mezzo non informatico, es. cercare un cartello che indichi qual è la rete Wi-Fi ufficiale, oppure consultare il titolare).
In ogni caso, se collegati a reti Wi-Fi esterne, si raccomanda:

- se si ha la necessità di scambiare informazioni riservate, assicurarsi che il canale di comunicazione usato sia ragionevolmente sicuro (es. uso di siti il cui indirizzo che compare nell'apposita barra del browser inizi per "HTTPS:\\");
- non effettuare transazioni bancarie;
- disabilitare la funzione di connessione automatica alle reti Wi-Fi.

3. PROTEZIONE DA VIRUS E GESTIONE VULNERABILITÀ DEI SISTEMI: ANTIVIRUS E AGGIORNAMENTI

Virus e malware, ovvero quei software che compiono azioni indesiderate, sono tra le principali cause di perdita dei dati e di malfunzionamento dei dispositivi.
Inoltre, i nuovi virus agiscono spesso in modo silenzioso con le seguenti finalità:

- permettere l'accesso ai dati, contenuti nei dispositivi, a persone non autorizzate;
- permettere azioni illegali in rete attraverso il vostro dispositivo;
- propagare le predette azioni dannose su altri dispositivi.

Molti degli attacchi informatici sfruttano eventuali falle di sicurezza (bug) presenti nei software installati e non ancora aggiornati oppure la cattiva prassi di utilizzare un account utente con privilegi di amministratore anche quando non sia necessario.

Raccomandazioni:

- assicurarsi che i dispositivi siano dotati di software antivirus;
- effettuare almeno mensilmente la scansione antivirus dell'intero sistema mediante l'antivirus installato (qualora il suddetto non la esegua automaticamente);
- se l'antivirus segnala file infetti, procedere sempre al blocco. Eventualmente i file fossero dei falsi positivi oppure risultassero bloccati software o file utili all'attività lavorativa, sbloccarli dall'interno dell'antivirus. In caso di dubbi chiedere supporto;
- nell'utilizzo della posta elettronica, non aprire mai allegati se non previo accertamento circa la loro reale provenienza. È possibile ricevere email solo apparentemente inviate da mittenti conosciuti, in realtà inviate da altri soggetti oppure da dispositivi infetti da malware senza che il mittente ne sia a conoscenza. In caso di email sospetta, si consiglia di contattare il mittente o richiedere supporto prima di aprire eventuali allegati;
- evitare il collegamento di dispositivi rimovibili (usb key, hard disk esterni, ecc.) senza una previa scansione mediante l'antivirus;
- attivare gli aggiornamenti automatici di applicazioni, dell'antivirus e del sistema operativo ed applicarli senza interromperne l'esecuzione (al limite rimandarla, se il software lo consente, qualora risultasse bloccante per l'attività lavorativa);
- non installare mai software di dubbia provenienza, soprattutto se viene richiesto con appositi messaggi durante la navigazione in rete;
- non utilizzare profili utente con privilegi di amministrazione se non è strettamente necessario. In tal caso porre particolare attenzione alle operazioni compiute.

Nel caso in cui, malgrado ogni prevenzione, si assista a comportamenti anomali del dispositivo come, ad esempio, il cambiamento di tutte le estensioni dei file e la comparsa di avvisi con richieste di pagamento, spegnerlo immediatamente. Nel caso si rendesse necessaria la riaccensione prima della verifica da parte di un tecnico, scollegare il cavo di rete o disabilitare il Wi-Fi prima della riaccensione.

4. DIFESA DAL PHISHING

Il "Phishing" è una tecnica di ingegneria sociale usata per effettuare delle truffe online. Come suggerisce il termine inglese, tramite delle "esche", generalmente delle e-mail trappola, dei malintenzionati inducono le potenziali vittime a credere di essere in contatto con altri soggetti fidati (Uffici dell'Università, amici, colleghi, parenti, banca, social, siti d'intrattenimento, siti di commercio

elettronico, etc.) al fine di farsi comunicare con l'inganno ("pescare"), credenziali di accesso, dati finanziari o altri dati personali. Di seguito alcuni esempi di email di Phishing:

Oggetto:
Da: "Universita' del Salento" <supporto.helpdesk@unisalento.it>
Data: Mer, 8 Ottobre 2016 12:23 am
A: undisclosed-recipients:;

*** Attenzione ***

Gentile utente, c'è stato un aggiornamento di sicurezza automatica sul Università sistema Adminstrative Server, prega di utilizzare il direct collegamento qui sotto per convalidare il tuo account WebMail.

CLICCA QUI:
http://webmial-hepdesk-confrm-mailverfy.2f.co/unisalento.it/confirm/webmail/

Copyright © 2015 Universita 'del Salento. Tutti i diritti riservati
supporto-helpdesk@unisalento.it
Help Desk supporto

From: Università del Salento <customercareservices15@outlook.com>
Subject: Università del Salento
Date: 11 maggio 2017 11:30:11 GMT+02:00
To: undisclosed-recipients:;

Caro abbonato !!
Stiamo attualmente conducendo un processo di manutenzione di tutti gli account e-mail. Per completare questo, si dovrà rispondere a questa email immediatamente e utilizzare il link sottostante per convalidare il tuo account contro spy-ware e e-mail spam.
Clicca qui per aggiornare

Questo processo ci aiuterà a combattere contro spam mail. La mancata per aggiornare l'account nel link qui sopra, renderà il vostro indirizzo e-mail attivo nel nostro database.
Grazie per la comprensione

Cordiali Saluti,
Webmail.unsalento.it
Account Management Service Team
Grazie per la tua collaborazione.

Raccomandazioni:

- diffidare di qualunque e-mail che richieda l'inserimento di credenziali di accesso o di dati personali. L'Ateneo, in particolare, non richiede mai credenziali di accesso (ad es. al servizio di posta elettronica) attraverso e-mail. Non comunicare i dati richiesti, evitare di aprire eventuali allegati o di cliccare sui link proposti. In caso di dubbi chiedere supporto o contattare il presunto mittente;

- per accedere all'applicazione webmail digitare l'URL direttamente nella barra degli indirizzi del vostro browser o raggiungerlo attraverso i vostri "preferiti" o "segnalibri" e non attraverso eventuali link proposti nelle e-mail.

5. NAVIGAZIONE CONSAPEVOLE IN RETE

La navigazione Internet è oramai uno degli strumenti indispensabili per l'attività lavorativa.
Allo stesso tempo, però può rappresentare un pericolo: navigare in un sito poco raccomandabile o comunque infetto può significare consegnare virtualmente il nostro dispositivo nelle mani di un malintenzionato.

Raccomandazioni:

- non procedere all'apertura di siti di dubbia provenienza, palesemente illegali o quando il browser, il sistema operativo o l'antivirus notificano possibili problemi di sicurezza; molti di questi siti potrebbero essere utilizzati per diffondere virus e malware;
- controllare sempre la barra degli indirizzi per verificare che il sito visitato sia autentico. Talvolta, infatti, per la diffusione di virus o per attività di phishing vengono usati siti fraudolenti con nomi simili a quelli originali, (es. www.googgle.com invece di www.google.com);
- purtroppo anche i cosiddetti pop-up (finestre di avviso o messaggi che si aprono automaticamente) possono essere veicoli di gravi minacce per il computer, quindi:
    - attivare il blocco dei pop-up nei browser utilizzati;
    - fare sempre attenzione alla richiesta di attivazione di pop-up. In caso di dubbi, prima di attivarli chiedere supporto;
    - fare attenzione a ciò che il browser condivide in rete: se non si è esperti di configurazioni del browser, chiedere supporto.

6. SCELTA, CUSTODIA E MODIFICA DELLE PASSWORD

La corretta gestione delle credenziali di accesso alle risorse elettroniche costituisce uno degli strumenti fondamentali per la protezione da attacchi informatici che mettono a rischio la sicurezza delle informazioni. In particolare, password scelte senza particolari accorgimenti o mal custodite espongono al rischio che altri possano accedere ai nostri dati o compiere azioni a nostro nome. Di seguito alcune raccomandazioni da seguire:

Raccomandazioni:

- adottare le necessarie cautele per assicurare la segretezza delle password: non comunicare mai ad altri le proprie password; non inviare via email nessuna password; nel digitare la password, fare attenzione ad eventuali sguardi indiscreti; non trascrivere le password su supporti cartacei o digitali non opportunamente custoditi;
- non lasciare incustodito e accessibile il personal computer: usare sempre una password a protezione dell'accesso al Sistema Operativo; abilitare sempre il salvaschermo e dotarlo di blocco temporizzato e sbloccabile con password;
- scelta delle password: scegliere password lunghe almeno 8 caratteri contenenti preferibilmente lettere maiuscole, minuscole, numeri e caratteri speciali (es.*,-,?, ecc.). Non usare password banali (es. "password", "1234" o "qwerty", ecc.) o comunque contenenti riferimenti agevolmente a voi riconducibili (ad es. nome, cognome, data e luogo di nascita, numero di telefono, codice fiscale, ecc.) . Gli hacker usano sistemi automatici e dizionari elettronici per trovare tantissime password in pochi secondi. Evitare quindi di utilizzare nomi di persone, cose o animali, anche se seguiti da numeri o simboli speciali: non è una complessità sufficiente;
- modifica delle password: modificare le password almeno una volta l'anno, quelle utilizzate per il trattamento di dati personali almeno ogni sei mesi. In caso di trattamento di dati sensibili e giudiziari, modificare la password almeno ogni tre mesi. Cambiare immediatamente la password nel caso si sospetti non sia più segreta.

7. UTILIZZO DELLA SUITE GOOGLE

Tutti gli utenti dell'Università utilizzano la piattaforma Google per il servizio di posta elettronica e possono fruire (in base alla categoria di appartenenza) delle altre app messe a disposizione sulla stessa (Drive, Documenti, Fogli, Presentazioni ecc.)
L'accesso al proprio "spazio" personale sulla piattaforma Google da parte di terzi compromette la sicurezza di tutti i dati ivi presenti. Oltre alle raccomandazioni più generali sull'uso delle password di accesso riportare nel paragrafo precedente, si evidenziano le seguenti.

Raccomandazioni:

- prestare molta attenzione alle email di avviso che Google invia agli utenti quando sono stati rilevati accessi sospetti (ovviamente prestare sempre attenzione alle email di phishing);
- in tal caso, e comunque periodicamente, controllare gli indirizzi IP degli ultimi dispositivi tramite i quali l'account si è connesso e verificare quali applicazioni stanno utilizzando il tuo account;
- impostare l'autenticazione a due fattori ove possibile.

8. COPIE DI SICUREZZA (BACKUP)

Il backup è quel processo che produce una copia, in una diversa location, dei file presenti sul dispositivo informatico. E' l'unico strumento che permette di non perdere definitivamente i dati qualora questi non siano più accessibili sul dispositivo, ad esempio a causa di un attacco informatico, della rottura del disco fisso, del furto o della distruzione del dispositivo, ecc.
In tutti questi casi, la presenza di una copia di backup permette di ripristinare l'operatività ed il patrimonio documentale, magari utilizzando un dispositivo differente.

Raccomandazioni:

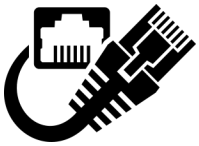
- effettuare almeno settimanalmente una copia di backup di tutti i dati (documenti, immagini, elementi multimediali etc.) necessari a ripristinare l'operatività della stazione di lavoro;
- assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La cifratura effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.

9. RACCOMANDAZIONI GENERALI

- Evitare di lasciare incustoditi e accessibili i dispositivi informatici, specie durante una sessione di lavoro che comporti trattamento di dati personali;
- al termine della sessione di lavoro sui server centrali, effettuare la procedura di disconnessione ("log off"/"log out"/"esci") ;
- spegnere il dispositivo se non è indispensabile, ad es. se non si è in servizio;
- effettuare la cifratura dei dati presenti nei dispositivi o di quelli particolarmente riservati se gli stessi vengono usati anche all'esterno degli edifici universitari;
- segnalare ai responsabili dei relativi servizi ogni sospetto di problema relativo a sicurezza o a privacy;
- in caso di dubbi, chiedere supporto

10. RACCOMANDAZIONI IN SINTESI

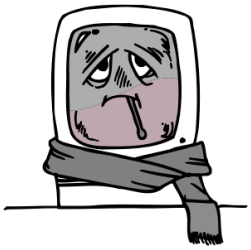
1. Scegli le connessioni più sicure



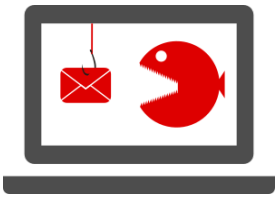
Privilegia la connessione via cavo ove possibile

2. Antivirus e Aggiornamenti

Usa un antivirus sempre aggiornato e applica gli aggiornamenti di sicurezza al sistema operativo e ai software installati. Fai attenzione ai dispositivi rimovibili e non usare privilegi di amministrazione se non necessario



3. Phishing



Non "abboccare" alle email in cui vengono chieste credenziali d'accesso e dati personali

4. Naviga consapevolmente

Evita siti sospetti, controlla gli indirizzi e disattiva di default i pop-up

5. Password

Sceglile e custodiscile con cura; cambiale periodicamente

6. Backup

Metti al sicuro i dati facendo delle copie periodiche di sicurezza su supporti esterni

7. Se hai dubbi...

….. o sospetti attacchi o infezioni da virus, chiedi supporto.