UNIVERSITÀ
DI SIENA
1240

UniSIcuri in Rete - ***Lavorare e studiare (anche smart) in sicurezza***

Dicembre 2020

Lavorare da remoto in sicurezza

La diffusione del virus SARS-CoV19 ha accelerato e amplificato l'utilizzo del lavoro "agile" ("*smartworking*" o "*lavoro da remoto*"), **attraverso l'utilizzo dei dispositivi personali degli utenti**. Anche la didattica ha dovuto affrontare la sfida della partecipazione da remoto, attraverso l'uso di tecnologie per permettere agli studenti di seguire le lezioni e affrontare esami da casa.

Il massiccio utilizzo delle tecnologie informatiche per le attività di studio e di lavoro porta con sé **la necessità di una maggiore consapevolezza di quali sono i rischi e le minacce informatiche**: i dati confermano che i cybercriminali stanno approfittando della situazione per portare avanti, talvolta con successo, i loro attacchi.

👉 Lavorare o studiare da remoto richiede maggiore consapevolezza dei rischi e delle minacce *cyber* a cui si può andare incontro

L'Agenzia per l'Italia digitale (AgID), attraverso il suo *Computer Emergency Response Team* (CERT) - https://cert-agid.gov.it/ - ha diffuso **linee guida e suggerimenti per lavorare e studiare in sicurezza** da remoto, senza mettere a rischio né i dati aziendali né quelli personali.

Analizziamo gli 11 punti del vademecum "*lavorare online in sicurezza*".

Smart working:
il vademecum per lavorare online in sicurezza

AGID | Agenzia per l'Italia Digitale

1 - La *Policy* di Ateneo

L'Università di Siena ha emanato, contestualmente ai decreti per l'aumento del lavoro agile come previsto dalle normative nazionali, una "*Informativa sulla sicurezza informatica*" a cui il personale dipendente è tenuto ad attenersi.

L'informativa è scaricabile dal sito web dell'Università di Siena, a questo URL: https://www.unisi.it/sites/default/files/allegatiparagrafo/informativa%20sicurezza%20informatica.pdf.

In tale documento si fa riferimento alla necessità di utilizzare dispositivi e pratiche conformi alle "**Misure minime di sicurezza ICT per le PA**" (https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict), oltre all'obbligo di utilizzare gli strumenti accesso remoto (VPN) per l'accesso ai dati di proprietà dell'Ateneo, evitando di farli uscire dal perimetro istituzionale.

"Perimetro istituzionale" è una definizione importante, perché identifica una zona, la Rete di Ateneo, dove **tutto il traffico in entrata e in uscita è controllato e protetto** da sistemi *antivirus*, IPS e *antimalware*. Anche se non è possibile rilevare e bloccare tutte le minacce, questi sistemi - *se affiancati dalle altre misure di sicurezza previste dalla normativa* - riescono a offrire un sufficiente livello di protezione.

👉 La VPN garantisce la sicurezza del traffico anche attraverso reti non sicure (es. *Hotspot pubblici*)

Per questo motivo **l'accesso ai dati e molti dei sistemi istituzionali è consentito solo previa connessione via VPN** (*Virtual Private Network*), uno strumento che permette di lavorare in modo analogo alla propria postazione all'interno della Rete di Ateneo.

È altresì importante che **su ogni dispositivo che si collega alla Rete aziendale, sia per lavoro che per studio, da locale o da remoto, sia installato, attivo e aggiornato un prodotto antivirus/antimalware** (*si può utilizzare Windows Defender oppure FortiClient*).

👉 Assicuratevi di **avere un valido prodotto antivirus e antimalware attivo** e aggiornato

---

È importantissimo che l'antivirus sia aggiornato, altrimenti potrebbe non riconoscere le minacce più recenti ed essere, pertanto, praticamente inutile.

Sconsigliamo inoltre l'utilizzo di prodotti antivirus gratuiti di terze parti, perché non sempre assicurano li

velli di protezione adeguati e, in certi casi, possono anche causare essi stessi problemi di sicurezza.

Nel malaugurato caso venga rilevata una infezione del sistema usato per lavorare su sistemi o su dati istituzionali, è importante segnalarlo via mail a helpdesk@unisi.it.

2 - Usare solo sistemi operativi supportati

Le "*Misure minime di sicurezza ICT per le PA*" richiedono che qualsiasi dispositivo informatico (*PC, smartphone, tablet...*) che gestisce dati o venga connesso alla Rete istituzionale abbia un sistema operativo supportato. È un fattore importante, perché **gli aggiornamenti di sistema garantiscono che i nostri strumenti informatici siano meno vulnerabili** a molti attacchi *cyber*. Per questo **è importante fare sempre gli aggiornamenti di sistema e usare solo sistemi operativi supportati.**

Molti attacchi ad aziende e istituzioni hanno successo **sfruttando le "falle" presenti in sistemi obsoleti e non aggiornati**: *non apriamo le porte ai cybercriminali!*

Ad esempio, per quanto riguarda **i sistemi Windows di Microsoft**, potete trovare l'elenco dei sistemi supportati a questa pagina: docs.microsoft.com/it-it/lifecycle/faq/windows

---

👉 Utilizzare **strumenti informatici non aggiornati** espone i tuoi dati, e i dati aziendali, a compromissioni e attacchi anche gravi.

---

3 - Proteggi i tuoi account e dispositivi

Proteggere **l'accesso al proprio PC, al proprio smartphone e a tutti gli altri servizi aziendali (e non) è di fondamentale importanza** per garantire la sicurezza dei nostri dati. È quindi importante:

- Impostare una **password sicura e strettamente personale** per ogni account utente (potete avvalervi di un password manager come KeePass: https://keepass.info);
- Se disponibile, **abilitare l'autenticazione a più fattori** (per la piattaforma Google: https://support.google.com/accounts/answer/185839)
- Sui PC portatili è importante **abilitare la cifratura del disco e usare una password sicura per accedervi**: in caso di furto o smarrimento, i dati personali e aziendali saranno al sicuro (su Windows 10 potete usare BitLocker, già incluso: https://support.microsoft.com/it-it/windows/crittografia-dispositivo-in-windows-10-ad5dcf4b-dbe0-2331-228f-7925c2a3012d)
- **Anche gli smartphone vanno protetti, con PIN numerico o password** all'accensione o per lo sblocco dopo un certo periodo di inattività;

- **Non comunicare mai ad altri, per nessun motivo, le proprie password**, neppure se la richiesta sembra lecita!

👉 Le credenziali di accesso ai dispositivi e ai dati (documenti, posta elettronica...) vanno protette e conservate con estrema cura.

In caso di **furto di credenziali o perdita di esclusività** (es. *la nostra password viene scoperta da terzi*) di accesso a dati o sistemi istituzionali deve essere immediatamente comunicata all'indirizzo abuse@unisi.it e, se opportuno, effettuare regolare denuncia alle autorità preposte (es. PolPoste).

4 - Non installare software illegale o non sicuro

Purtroppo c'è ancora **la pericolosa abitudine a utilizzare software scaricato illegalmente** ("*craccato*") o da fonti non sicure. Oltre a essere illegale, questo software è spesso veicolo di *malware* e *trojan* che potrebbero danneggiare il nostro PC e i dati in esso contenuti.

👉 Usare software "pirata" è pericoloso, oltre che illegale.

Ad esempio, **si stanno moltiplicando gli attacchi *ransomware*** che, veicolato proprio attraverso allegati o software "pirata", cifra tutti i documenti, rendendo inutilizzabile il sistema, per poi chiedere un riscatto pecuniario per ottenere la chiave di decifrazione: **le conseguenze di questi atti criminali sono molto pesanti**, con

aziende che si sono trovate bloccate nel processo di produzione (parliamo di realtà come *Luxottica*, *Enel...*) e con milioni di euro di riscatto da dover pagare.

È pertanto necessario fare particolare attenzione a ciò che scarichiamo e installiamo sui nostri PC o smartphone: le conseguenze possono essere molto gravi.

Quando si ha una particolare esigenza **è bene valutare se esistono prodotti *open source* adeguati**, senza spendere migliaia di euro in licenze o rischiare conseguenze ancora più gravi usandone una copia illegale.

5 - Occhio al *phishing*!

Il *phishing* è stato l'oggetto della nostra prima newsletter dedicata alla sicurezza, che potete trovare a questa pagina: www.uet.unisi.it/category/sicurezza/

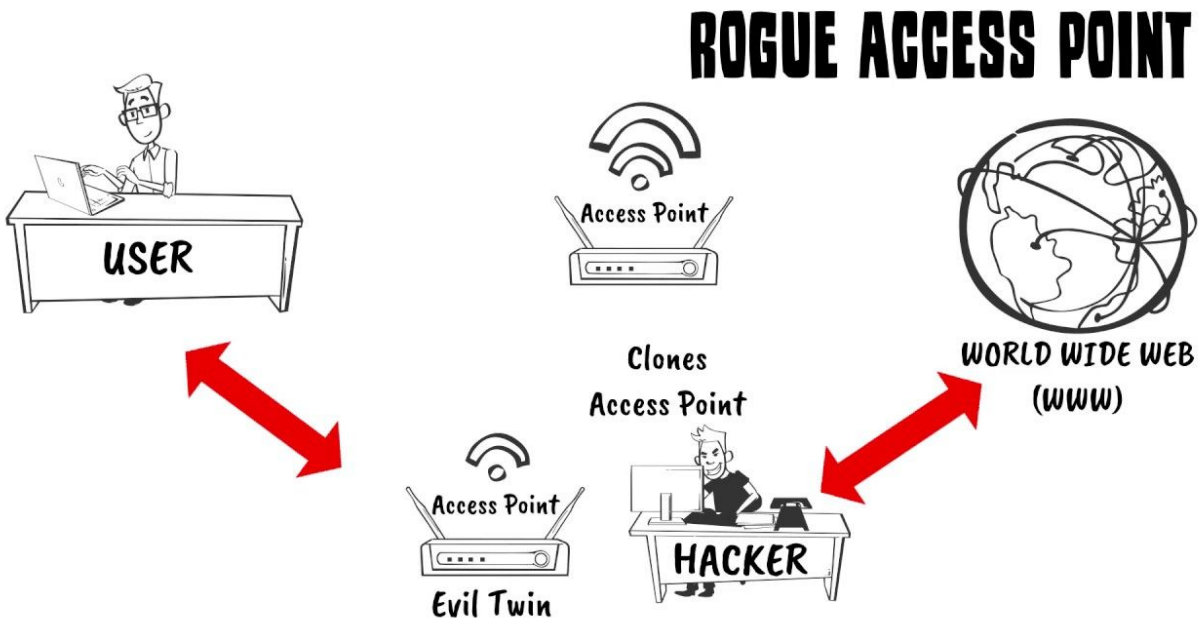
> 👉 Il *phishing* è ancora oggi il maggior veicolo di attacco utilizzato dai cybercriminali

Ricordiamo tuttavia l'importanza di **non "abboccare" alle tante mail e comunicazioni truffaldine che quotidianamente riceviamo via posta elettronica o SMS**: mai fornire le proprie credenziali senza prima essersi accertati della liceità della richiesta e aver verificato l'attendibilità del sito web.

6 - Solo connessioni sicure

Potrà sembrare banale ma l'utilizzo di connessioni sicure, in particolare WiFi, è di fondamentale importanza per evitare furti di identità e di dati. Assicuriamoci sempre che il punto di accesso WiFi al quale ci stiamo collegando sia sicuro ed **evitiamo l'utilizzo di hot-spot pubblici (es. La WiFi del Bar sotto casa) per operazioni delicate come acquisti in Rete o accesso all'Home Banking**: le nostre credenziali potrebbero essere rubate e usate da terzi in modo improprio!

👉 Non usare reti WiFi pubbliche per acquisti **on-line** o per accedere al vostro **home banking**



È un attacco piuttosto facile da realizzare e per questo è di fondamentale importanza fare particolare attenzione a quale connessione utilizziamo. Nel dubbio, **meglio usare la connessione 4G/LTE del proprio smartphone** che rischiare un *costoso* furto di credenziali...

7 - Ricordati il *logout*!

Chiudere il *browser* o spegnere il PC non significa automaticamente la disconnessione dalla propria sessione di lavoro. In molti casi, la sessione rimane "appesa" ed è possibile che qualche malintenzionato possa usufruirne per accedere ai vostri dati, o ai dati aziendali, a vostra insaputa.

Per questo **è importante, al termine della sessione di lavoro o di studio, chiudere esplicitamente il collegamento** cliccando su "Logout" o "Esci": un semplice gesto che evita conseguenze potenzialmente più gravi.

Riferimenti

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

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

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

- **Garante per la protezione dei dati personali** - Regolamento europeo in materia di protezione dei dati personali - www.garanteprivacy.it/regolamentoue
- **Agenzia per l'Italia digitale** - Glossario - *phishing* - cert-agid.gov.it/glossario/phishing/
- **Garante per la protezione dei dati personali** interviene sul *phishing* - www.garanteprivacy.it/temi/cybersecurity/phishing

Contatti e siti web utili

- Gestione delle **credenziali unisiPass** e **aggiornamento password**: my.unisi.it
- **Avvisi di sicurezza** dell'Università di Siena: www.uet.unisi.it/category/sicurezza/
- Servizio di **assistenza tecnica** Università degli Studi di Siena: helpdesk@unisi.it