MODULARIO
I. - *Ramo Pref.* - 4

Mod. 4

*Prefettura - Ufficio territoriale del Governo di Napoli*

Prot.(*vedasi stampigliatura laterale*) Area II Staff 1 Napoli, (*data del protocollo*)

*A mezzo posta elettronica certificata*

Ai Segretari Comunali e agli Ufficiali Elettorali
dei Comuni dell'Area Metropolitana di Napoli
LORO SEDI

CIRCOLARE N. 34/ AMM. REF. 2025

OGGETTO: Elezioni amministrative del 25 e 26 maggio e referendum abrogativi del 8 e 9 giugno 2025. Raccomandazioni per la sicurezza delle postazioni di lavoro informatiche dei Comuni.

Si fa seguito alle indicazioni fornite con circolare precedenti circolari, in merito alle modalità di inserimento nel Sistema centrale Siel dei dati elettorali e referendari ufficiosi.

Attesa la delicatezza degli imminenti eventi elettorali, il Ministero dell'Interno – Direzione Centrale per i Servizi Elettorali, con circolare n. 50/2025 ha richiamato l'attenzione sul pieno rispetto delle indicazioni fornite in merito alla gestione delle postazioni di lavoro, attraverso le quali viene consentito l'accesso al sistema SIEL per l'inserimento dei dati.

Come è noto, ciascun comune è tenuto ad osservare le prescrizioni indicate dall'Agid per la sicurezza ICT delle pubbliche amministrazioni (https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict ).

Al fine di innalzare il livello di sicurezza delle postazioni utilizzate per l'inserimento dati, la predetta Direzione Centrale ha fornito le allegate raccomandazioni redatte in collaborazione con l'Agenzia per la Cybersicurezza Nazionale, nell'ottica di prevenire efficacemente eventuali rischi di natura informatica.

Le SS.LL. vorranno assicurare a vista la necessaria sensibilizzazione del personale interessato sulla necessaria e pronta adozione delle presenti misure di sicurezza ICT.

Pertanto, s'invitano le SS.LL. a porre in essere ogni misura organizzativa consentita ad adempiere a quanto richiesto, che riveste fondamentale rilevanza per la corretta diffusione dei risultati ufficiosi delle prossime consultazioni amministrative e referendarie.

Il Dirigente dell'Ufficio elettorale provinciale
Vice Prefetto
( Esposito)

*Area II Staff 1 - Raccordo con gli Enti locali – Consultazioni elettorali*
*Piazza del Plebiscito n. 22 – 80132 Napoli*
Pec: *elettorale.prefna@pec.interno.it*

**Raccomandazioni generali**

- Rispetta le regole definite nel disciplinare per l'utilizzo di tutti gli strumenti informatici rilasciato dalla tua amministrazione.
- Utilizza la postazione di lavoro esclusivamente per le attività strettamente legate all'attività dell'amministrazione.
- Assicurati che vengano periodicamente installati gli aggiornamenti di sicurezza sul sistema operativo e su tutto il software utilizzato sulla macchina.
- Verifica che sul PC siano attivi i software di protezione (antivirus, firewall ecc.) e che le firme siano costantemente aggiornate.
- Cambia la password di accesso al pc periodicamente.
- Assicurati che l'accesso alla postazione sia protetto da una password robusta conforme alle policy dell'amministrazione. Un utile riferimento è rappresentato dalla versione 4.0 del documento OWASP ASVS (Application Security Verification Standard) che suggerisce per le password degli utenti una lunghezza minima di 12 caratteri.
- Disconnetti o blocca la sessione utente prima di lasciare incustodita la postazione. Questa raccomandazione diventa ancora più importante quando la policy dell'amministrazione non prevede la disconnessione automatica dopo un periodo di inattività.
- Non salvare password all'interno di file non cifrati o su documenti cartacei incustoditi.
- Utilizza un gestore password, possibilmente off line per memorizzare e generare le credenziali di applicazioni che gestiscono dati sensibili.
- Esegui il log out dagli applicativi al termine dell'attività lavorativa. Evita in generale di rimanere loggato su più applicativi se non strettamente necessario.
- Non installare software non consentiti dalle policy e/o provenienti da fonti non ufficiali.
- Per le postazioni mobili, utilizza l'accesso a connessioni Wi-Fi adeguatamente protette e consentite dalle policy.
- Se consentito dalle policy dell'amministrazione, utilizza pen drive o hard disk esterni solo se di sicura provenienza.
- Denuncia immediatamente lo smarrimento o il furto di qualsiasi bene informatico legato all'attività lavorativa in modo che l'amministratore IT possa disabilitare tale dispositivo, evitando così possibili accessi abusivi che potrebbero compromettere l'integrità dei dati e la reputazione della tua amministrazione.

**Accesso alle applicazioni e gestione delle password**

- Se l'applicazione lo prevede, utilizza l'autenticazione 2FA (2 factor authentication). Il multi factor authentication assicura che l'utente si identifichi con una combinazione dei seguenti fattori:
  - "Una cosa che sai", per esempio una password o il PIN

  - "Una cosa che hai", come uno smartphone o un token di sicurezza (ad esempio "chiavette" che forniscono un codice OTP).
  - "Una cosa che sei", cioè un dato biometrico, come l'impronta digitale, il timbro vocale, il viso o l'iride.
- Come secondo fattore di autenticazione preferisci se disponibili applicazioni OTP (One Time Password) o simili al posto di quella basata su SMS.
- Cambia la password di default degli applicativi o la password che ti viene assegnata al primo accesso.
- Non utilizzare le password che siano già state esposte in precedenti data leak. A tal proposito la lista delle 10000 password più usate pubblicata su Github da Seclists può essere di aiuto.

**Attività di navigazione web**

- Naviga sulla rete Internet solo se necessario alle attività d'istituto.
- Usa un browser aggiornato e assicurati che gli aggiornamenti di sicurezza vengano regolarmente installati.
- Usa differenti browser (es. Chrome e Firefox) per diverse tipologie di attività (es. uno per le applicazioni web di lavoro e uno per la navigazione) al fine di ridurre la superficie d'attacco.
- Non salvare le password all'interno del browser.
- Non installare estensioni nel browser, se non strettamente necessario. Queste aumentano la superficie d'attacco in quanto possono contenere codice malevolo. Anche le estensioni legittime più diffuse, potrebbero diventare un vettore d'attacco se il loro repository di codice sorgente (es. Gitlab, Github, ecc.) venisse compromesso.
- Non riutilizzare la stessa password su più piattaforme e applicazioni web di lavoro.
- Non utilizzare l'indirizzo mail di lavoro per la registrazione di utenze su portali web non appartenenti all'amministrazione.
- In tutte le fasi in cui vengono scambiati dati sensibili tra browser e sito web, assicurati che il protocollo utilizzato sia https. Per gli utenti più avanzati: verifica che non vengano utilizzati protocolli TLS e cifrari deprecati o non sicuri.
- dalle impostazioni di sicurezza delle applicazioni web:
  - controlla periodicamente le connessioni effettuate sugli applicativi web al fine di individuare eventuali accessi sospetti da device e/o IP non riconosciuti come legittimi.
  - disconnetti i dispositivi abilitati all'accesso quando non sono più utilizzati da molto tempo.

**Utilizzo di client e-mail e instant messaging**

- Utilizza client e-mail o sistemi di instant messaging solo se necessari per le attività di istituto.

- Non cliccare su link o allegati contenuti in e-mail sospette. In particolare, effettuare le seguenti verifiche:
  - il dominio non è correlato con l'azienda che ha inviato il messaggio;
  - il dominio è molto lungo;
  - il dominio contiene molti caratteri ' - ' (es. hxxps[:]//intesa-san-paolo-accesso- conto.dominio-fake.com);
  - il nome del brand è contenuto nel path (es. hxxp[:]//108.179.216.140/intesasanpaolo);
  - è presente una mail (es. hxxp[:]//username[@]hotmail.com.fddcol.com);
  - il nome del dominio è codificato (es. hxxps[:]//www[.]%64isc%72%65%74%2done-%6ei%67h%74.%63o%6d);
  - l'indirizzo IP è codificato (es. hxxp[:]//0x42.0x1D.0x25.0xC2);
  - sono presenti simboli provenienti da altre lingue simili all'alfabeto latino.
- Non cadere nelle truffe. I criminali sono diventati bravi nell'impersonare le persone a te più vicine sfruttando le tue informazioni personali disponibili online. Di seguito vengono descritte due tipologie di truffe e i comportamenti da adottare:
  - Truffe a tema "lotteria / premi": ignora e-mail / sms che ti comunicano di aver vinto un premio e ti viene chiesto di pagare una commissione o una tassa per ritirare il premio. Qui puoi vincere non cadendo in questa truffa.
  - Truffe del finto supporto tecnico: se qualcuno ti contatta per darti assistenza tecnica per un problema tecnico che non hai o per dispositivo che non possiedi, fermati subito e interrompi la comunicazione. È probabile che i truffatori impersonino amministratori IT della rete per ottenere l'accesso remoto al tuo computer o ai tuoi dati sensibili.
- Per aumentare la consapevolezza sulle tecniche di phishing e social engineering esistono molte risorse on line gratuite, come le seguenti messe a disposizione da note organizzazioni pubbliche e private:
  - https://teamdigitale.github.io/security-awareness/episodes
  - https://phishingquiz.withgoogle.com/
  - https://learnsecurity.amazon.com/training/story.html

**Riferimenti**


- https://learn.microsoft.com/it-it/lifecycle/faq/windows
- https://support.apple.com/it-it/109033
- https://www.cisa.gov/be-cyber-smart/common-scams
- https://github.com/OWASP/ASVS/blob/master/4.0/en/0x11-V2-Authentication.md
- https://github.com/OWASP/ASVS/blob/master/4.0/en/0x11-V2-Authentication.md
- https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/darkweb2017_top-10000.txt