LOGO COMUNE

LINEE GUIDA PER LA NAVIGAZIONE SICURA WEB IN MODALITA' COMPLIANCE DELL'ENTE LOCALE

Generalità

Qui di seguito vengono indicati alcune linee guida, best practice da utilizzare nella navigazione web sicura da parte dei dipendenti dell'ente locale secondo i principi di accountability, compliance, privacy by default e privacy by design previsti dal vigente Regolamento UE 679/2016 (GDPR).

Gran parte dei pericoli per la sicurezza del proprio computer vengono corsi durante la navigazione in internet. Molti di questi pericoli possono essere evitati adottando opportune misure comportamentali che vengono riportate di seguito.

- **non scaricare programmi sconosciuti** - Non scaricare mai programmi sconosciuti da internet prima di averne accertato la provenienza
- **aggiornamento del software dai siti dei produttori** Scaricare gli aggiornamenti di software e driver esclusivamente dalla pagina web dei relativi produttori. È sempre buona norma anche verificarli successivamente con un programma antivirus aggiornato
- **prudenza nella trasmissione di informazioni** Non comunicare mai a nessuno le proprie credenziali di accesso (nome di utente e password). Nessun fornitore di servizi serio chiederà la vostra password (nemmeno telefonicamente). Questo vale anche quando la richiesta appare credibile. Tale garanzia è riconoscibile da un lucchetto dorato che appare all'interno del browser oppure dal protocollo utilizzato (tipicamente "https" invece di "http")
- **chiudere le applicazioni** - Utilizzare sempre l'apposita notifica di chiusura ("logout") quando si esce da un'applicazione web che abbia richiesto l'introduzione delle proprie credenziali di accesso
- **riservatezza nella divulgazione delle informazioni personali** Evitate di rivelare dati personali durante la compilazione di moduli Web o la fornitura di contributi a newsgroup, forum o registri di visitatori
- **attenzione alla configurazione del browser** Molte delle minacce che si incontrano durante la navigazione in internet sono legate all'utilizzo dei componenti "dinamici" delle pagine web tipicamente realizzati tramite controlli ActiveX o funzioni JavaScript. Tali funzionalità sono spesso indispensabili per il corretto funzionamento della pagina, ma spesso vengono utilizzate in maniera malevola da parte di malintenzionati per il lancio di malware sulla macchina ospite. Una possibile contromisura può essere la limitazione di JavaScript o dei ActiveX:
    - provare a limitare o a disattivare l'esecuzione di JavaScript mediante la configurazione del browser. Va però osservato che in caso di disattivazione di JavaScript numerose pagine Web non funzionano più correttamente. In tal caso è possibile allentare gradualmente le limitazioni sino a un livello minimo di funzionalità
    - provare a limitare nella misura del possibile l'esecuzione dei controlli ActiveX mediante la configurazione del navigatore.
    - Mantenere tendenzialmente le opzioni di sicurezza automatiche (per la configurazione delle quali si rimanda alla documentazione del browser che si utilizza) sul valore "alto".

Sensibilizzare il personale sui rischi che la navigazione in Internet via Browser comporta

Di seguito le principali norme comportamentali da seguire:

- Non fare clic su collegamenti senza considerare i rischi che ne potrebbero derivare (evitare di cliccare su link sospetti presenti nelle pagine).
- Prestare attenzione al fatto che gli indirizzi di pagine Web potrebbero essere mascherati e

portare in un sito imprevisto.

- Considerare che ogni volta che un sito web richiede che vengano abilitate determinate funzionalità o installati software e aggiornamenti, si mette a rischio il computer. Ad es. non aggiornare mail il Flash Player su richiesta di una pagina web ma solo da pannello di controllo.
- Non riutilizzare la stessa password per siti diversi.
- Non fornire mai online informazioni personali a meno di non essere certi che il sito sia valido e le transazioni sicure: prima di inserire qualsiasi informazione personale, controllare la barra degli URL del browser al fine di accertarsi che il sito sia quello atteso e che sia presente la dicitura "https:" e un'icona a forma di lucchetto ad indicare che la connessione al sito è protetta e che il certificato server è valido.
- Evitare Wi-Fi pubblici o gratuiti: l'attaccante spesso utilizza sniffers wireless per rubare le informazioni degli utenti quando vengono inviate su reti non protette. Il modo migliore per proteggersi da questo attacco è evitare di utilizzare queste reti, oppure utilizzarle solo con una VPN che incapsuli tutto il traffico in un tunnel cifrato.
- In caso di individuazione di una "falsa" pagina di autenticazione segnalarla tempestivamente all'Assistenza Tecnica dell'ente in sinergia con l'Ufficio CED Sistemi Informativi Comunale per procedere all'oscuramento della medesima e possibilmente all'individuazione dei responsabili.

Hardening del browser (l'insieme di operazioni specifiche di configurazione del software di navigazione web (e dei suoi relativi componenti) che mirano a minimizzare l'impatto di possibili attacchi informatici che sfruttano vulnerabilità dello stesso, migliorandone pertanto la sicurezza complessiva). Di seguito alcuni accorgimenti tecnici da seguire:

- **Attivare il blocco dei popup del browser**. Le finestre di popup sono una notevole tecnica di "phishing". Il blocco dei popup è oggi una funzionalità standard dei browser e dovrebbe essere abilitato ogni volta che si naviga sul web. Può essere utilizzata anche su siti web specifici e non su altri, dove i popup potrebbero invece essere necessari.
- **Disabilitare la memorizzazione di password nel browser**. Quasi tutti i browser e molti siti web in genere offrono la possibilità di ricordare le password per uso futuro. L'attivazione di questa funzionalità memorizza le password in un'unica posizione sul computer, rendendo più facile per un aggressore scoprirle se il sistema venisse compromesso. Se questa funzionalità risulta abilitata, è necessario disattivarla e cancellare le password memorizzate.

Privacy durante la navigazione web

Adottare le seguenti misure a salvaguardia della privacy degli utenti, rispetto ai siti Web che monitorano le attività utente:

- **Impostare una routine specifica** per eliminare i cookie regolarmente. Alcuni cookie possono costituire un rischio per la privacy in quanto tengono traccia dei siti visitati. Non sempre è possibile bloccare i cookie, ma è opportuno eliminarli (diversamente i cookie possono rimanere memorizzati nel sistema per settimane o più)
- **Attivare funzionalità "Do Not Track**". "Do Not Track" è un header HTTP che comunica ai siti visitati e alle terze parti i cui contenuti sono ospitati in tali siti che le proprie attività non devono essere tracciate. **Nota Bene.** L'invio di una richiesta "Do Not Track" ai siti non garantisce la protezione della privacy. I siti possono scegliere di rispettare la richiesta o continuare a eseguire attività che potrebbero essere considerate di monitoraggio anche se è stata espressa questa preferenza.
- **Utilizzare la navigazione anonima**. **Nota Bene**. Il livello di protezione è diverso a seconda dei browser. In certi casi si tratta di una difesa da attacchi locali: alcune info, come le password, la cronologia di ricerca e la cronologia delle pagine, vengono eliminate alla chiusura della scheda. In altri casi si tratta della difesa dall'attaccante esterno ossia viene

protetto l'**anonimato durante la navigazione**.

- **Disattivare la condivisione della posizione geografica**

Hardening del browser: configurazione di base per la sicurezza

La configurazione di default per molti browser web non è sicura. Si raccomandano i passaggi a seguire per rendere maggiormente sicuro il browser web in uso. Tali impostazioni assumono particolare importanza nel caso in cui si utilizza il browser per accedere a sistemi dell'Ente Locale o più in generale se si utilizza il browser per accedere, inviare o ricevere informazioni sensibili.

1. **Impostare il browser di default:**
   - Firefox: sia per Mac che per Windows - andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > scheda Generale. Selezionare la casella "Controlla sempre se Firefox è il browser predefinito".
   - Safari: andare nel menu Safari > Preferenze > scheda Generale e clicca sul pulsante "Imposta predefinito".
   - Internet Eplorer: si raccomanda di non utilizzare IE come browser predefinito.
   - Google Chrome: andare sulle impostazioni nella sezione "Browser predefinito" e cliccare sul pulsante "Imposta come predefinito" in corrispondenza della voce "Imposta Google Chrome come browser predefinito".
2. **Mantenere il software del browser aggiornato**.
3. **Abilitare nel browser gli aggiornamenti automatici e mantenerli in tale stato:**
   - Firefox: sia per Mac che per Windows - vai al menu Firefox > Preferenze (Mac), scheda Opzioni (Windows), scheda Generale > sezione Aggiornamenti di Firefox. Selezionare "Installare automaticamente gli aggiornamenti (consigliato)".
   - Safari: gli aggiornamenti in Safari sono gestiti nel menu Apple in Preferenze di sistema > Aggiornamento software. Impostare su Aggiornamenti giornalieri.
   - Google Chrome: a garanzia di protezione, Google Chrome si aggiorna automaticamente ogni volta che rileva che è disponibile una nuova versione del browser. Il processo di aggiornamento avviene in background e non richiede alcuna azione manuale.
4. **Bloccare l'accesso ai pop-up, plug-in e ai siti di phishing:**
   - Firefox: per il blocco dei pop-up indesiderati, sia per Mac che per Windows - andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > sezione Permessi. Selezionare "Blocca le finestre pop-up".
   - Firefox: per il blocco delle estensioni del browser indesiderate, sia per Mac che per Windows - andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > sezione Permessi. Seleziona "Avvisa se un sito web tenta di installare un componente aggiuntivo".
   - Safari: per il blocco dei pop-up indesiderati, andare nel menu Safari > Preferenze > scheda Siti web, fare clic su "Finestre di pop-up" dal pannello di sinistra e impostare "Quando si visitano altri siti web:" su "Blocca e notifica".
   - Safari: per il blocco del phishing e delle estensioni del browser indesiderate, andare nel menu Safari > Preferenze > Scheda Siti Web e deselezionare i plug-in installati indesiderati presenti nel pannello di sinistra.

- Edge: per il blocco dei pop-up indesiderati, andare su Impostazioni > Impostazioni avanzate > Blocca popup e impostarlo a Attivato.
- Internet Explorer: per il blocco dei pop-up indesiderati, andare nel menu Strumenti > Opzioni Internet > scheda Privacy. Selezionare la casella di controllo "Attiva Blocco popup".
- Internet Explorer: per il blocco delle estensioni del browser indesiderate, andare nel menu Strumenti > Opzioni Internet > scheda Avanzate e scorrere verso il basso fino a "Elementi multimediali". Deselezionare se selezionate, "Riproduci animazioni" e "Riproduci suoni" in pagine web.
- Google Chrome: per il blocco dei pop-up indesiderati, andare su Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Pop-up e reindirizzamenti e impostare su "Bloccato".
- Google Chrome: per il blocco delle estensioni del browser indesiderate, andare su Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Accesso al plugin senza sandbox e impostare su "Chiedi conferma quando un sito vuole utilizzare un plug-in per accedere al tuo computer (opzione consigliata)".

5. **Impostare il browser in modo tale da non salvare le password.** Diversamente se strettamente necessario, utilizzare un meccanismo di master password conforme allo standard UCSC (https://its.ucsc.edu/security/password.html):
    - Firefox: sia per Mac che per Windows - andare nel menu Firefox >Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > sezione Privacy del browser > Credenziali e password. Deselezionare la casella di controllo "Chiedi se salvare le credenziali di accesso ai siti Web".
    - Firefox: per l'utilizzo di una master password, se è necessario salvare le password, impostare una password Master in modo che le password salvate non siano facilmente accessibili a chiunque abbia accesso al sistema. Sia per Mac che per Windows- andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > sezione Privacy del Browser > Credenziali e password. Selezionare "Utilizza una password principale".
    - Safari: andare nel menu Safari > Preferenze > Scheda Riempimento automatico e deselezionare la casella "Nomi utente e password".
    - Edge: andare nel menu Impostazioni > Impostazioni avanzate > Privacy e servizi > "Offri la possibilità di salvare le password" e impostare a Disattivato e "Salva i dati immessi nei moduli" a Disattivato.
    - Internet Explorer: andare nel menu Strumenti > Opzioni Internet > Scheda Contenuto e fare clic sul pulsante Impostazioni di "completamento automatico" e deselezionare la casella "Nome utente e password sui moduli".
    - Internet Explorer: IE non ha una funzione master password, ma sarebbe opportuno disabilitare la funzione di completamento automatico per le password. Vedere l'indicazione precedente.
    - Google Chrome: andare nel menu Impostazioni > Compilazione automatica > Password e disattivare "Chiedi di

salvare le password".

6. **Disabilitare i third-party cookie.**
   - Firefox: sia per Mac che per Windows - andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > Blocco contenuti. Seleziona "Personalizzato" e imposta i cookie per bloccare "Traccianti di terze parti". Abilitare anche i controlli per bloccare i criptominer e le Fingerprinter.
   - Edge: andare nel menu Impostazioni > Impostazioni avanzate > "Privacy e servizi" quindi attivare "Invia richieste Do Not Track", disattivare "Mostra suggerimenti per la ricerca e i siti durante la digitazione", impostare i Cookie su "Blocca solo i cookie di terze parti", disattivare "Usa la previsione della pagina per velocizzare l'esplorazione, migliorare la lettura e migliorare l'esperienza nel complesso" e abilitare "Proteggi il PC da siti e download dannosi con il filtro SmartScreen".
   - Internet Explorer: andare nel menu Strumenti > Opzioni Internet > scheda Privacy e fare clic sul pulsante "Avanzate". Selezionare la casella "Accetta" per i cookie dei siti Web visualizzati e il pulsante "Chiedi conferma" per i cookie di terze parti. Il pulsante "Accetta sempre i cookie della sessione" non dovrebbe essere selezionato. Fare clic su OK. Al termine, fare clic sul pulsante Applica.
   - Google Chrome: andare nel menu Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Cookie > e attivare "Consenti ai siti di salvare e leggere i dati dei cookie (opzione consigliata)" e "Blocca cookie di terze parti".
7. **Impostazioni specifiche per tipologia di browser:**
   - Firefox: installare l'estensione del browser "uBlock Origin" per il blocco degli annunci.
   - Firefox: contenuto ingannevole e protezione da software pericoloso -sia per Mac che per Windows - andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > sezione Sicurezza. Spuntare "Blocca contenuti a rischio e ingannevoli", "Blocca download a rischio" e "Avvisa in caso di software indesiderato e non scaricato abitualmente".
   - Firefox: raccolta e utilizzo dei dati Firefox - sia per Mac che per Windows - andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > Raccolta e utilizzo dati di Firefox. Deselezionare "Consenti a Firefox di inviare a Mozilla dati tecnici e relativi all'interazione con il browser", "Consenti a Firefox di installare e condurre studi" e "Consentire a Firefox di inviare segnalazioni di arresto anomalo in sospeso".
   - Safari: disabilitare Java. Andare nel menu Safari > Preferenze > Scheda Sicurezza e impostare il segno di spunta per abilitare "Avvisa quando visiti un sito web fraudolento" e un segno di spunta per "Abilita JavaScript".
   - Safari: privacy - andare nel menu Safari > Preferenze > scheda Privacy e selezionare "Prevent cross-site tracking".
   - Safari: apertura in modo sicuro dei file scaricati - andare nel menu Safari > Preferenze > scheda Generale. Deselezionare la casella di controllo che indica "Open 'safe' files after downloading".

- Edge: disattivare Flash - andare nel menu Impostazioni > Impostazioni avanzate > "Usa Adobe Flash Player" e impostare su Disattivato.
- Internet Explorer: impostare le security zones, ovvero i livelli di sicurezza per le aree "Internet", "Intranet locale", "Siti attendibili" e "Siti con restrizioni".
- Internet Explorer: disattivare il filtro ActiveX - aprire IE, premere il tasto Alt, aprire il menu Strumenti, e cliccare su "ActiveX Filtering", se non è già spuntato.
- Internet Explorer: suggerimenti aggiuntivi - IE dispone di zone di sicurezza che possono essere impostate per diversi livelli di protezione. Aprire IE, premere il tasto Alt, aprire il menu Strumenti, e cliccare su "Opzioni Internet", selezionare la scheda "Sicurezza". Si consiglia di impostare il livello di sicurezza per l'area "Internet" su ALTA. È inoltre possibile identificare i "Siti attendibili" e impostarli su MEDIO-ALTA.
- Google Chrome: andare nel menu Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > JavaScript e attivare "Consentita (opzione consigliata)".
- Google Chrome: fare in modo che per l'esecuzione di contenuti Flash venga chiesto il consenso - andare nel menu Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Flash > e impostare su "Chiedi prima".
- Google Chrome: download automatici - andare in Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Download automatici e impostare su "Chiedi conferma quando un sito tenta di scaricare automaticamente file dopo il primo file (opzione consigliata)".
- Google Chrome: accesso alla videocamera - andare nel menu Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Videocamera e impostare su "Chiedi prima di accedere (opzione consigliata)".
- Google Chrome: accesso al microfono: andare nel menu Impostazioni Avanzate > Privacy e sicurezza > Impostazioni sito > Microfono e impostare su "Chiedi prima di accedere (opzione consigliata)"