Trasmissione a mezzo posta elettronica ai sensi dell'art.47 del D. Lgs n. 82/2005

r_puglia/AOO_174/PROT/29/10/2021/0006728

A tutto il personale della Regione Puglia

LORO SEDI

Oggetto: Buone pratiche per la sicurezza informatica

La sicurezza informatica è un tema complesso che necessita di adeguate soluzioni organizzative e tecnologie e richiede la collaborazione di ciascun singolo utente.

Sempre più spesso, infatti, alcuni comportamenti degli utilizzatori facilitano gli attacchi anche a sistemi informativi che offrono un elevato livello di sicurezza.

È, quindi, necessario che il comportamento degli utilizzatori non generi situazioni di pericolo tali da ridurre la sicurezza intrinseca di un sistema, mettendo in pericolo sia il sistema, che i dati che esso gestisce.

Per contrastare e prevenire efficacemente gli "attacchi informatici" è, quindi, necessario che **tutto il Personale della Regione Puglia** adotti delle "buone pratiche di utilizzo dei sistemi" che sono riassunte nel documento allegato.

Cordialmente,

Il Responsabile per la Transizione al Digitale
Ing. Cosimo Elefante

REGIONE PUGLIA
Elefante Cosimo
29.10.2021
20:34:40
GMT+00:00

Ufficio per la transizione al Digitale
Lungomare Nazario Sauro, 33 - 70123 Bari – tel. 080 540 3727 – 080 540 6918
resp.transizionedigitale@regione.puglia.it
resp.transizionedigitale@pec.rupar.puglia.it

BUONE PRATICHE PER LA SICUREZZA INFORMATICA

GESTIONE DELLE CREDENZIALI

Scelta della password

- la password deve essere cambiata almeno ogni 3 mesi;
- la password deve essere composta da almeno otto caratteri, oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la password non deve contenere riferimenti aventi attinenza con la vita privata o professionale facilmente riconducibili all'utente (evitare ad es. nome, cognome, data di nascita, numero di telefono, codice fiscale, luogo di nascita, nome di parenti, figli, cane, etc.);
- le password non dovrebbero essere parole di senso comune presenti sul dizionario;
- la password non deve contenere una serie consecutiva di soli numeri o di sole lettere;
- la password, nel caso in cui lo strumento elettronico lo permetta, deve essere preferibilmente composta da una sequenza di lettere, numeri e caratteri speciali (es. di caratteri speciali: &;@*§ ? % £=@ $);
- la password non deve essere costituita da una sequenza ovvia sulla tastiera (es. qwerty, 123456);
- la password deve essere diversa dalle ultime 5 password utilizzate;
- la password deve essere diversa per ciascun applicativo/software/device che ne richieda una.

Cautele per la segretezza della password

- utilizzare sempre esclusivamente le proprie credenziali di autenticazione;
- non condividere la propria password con altri colleghi;
- mantenere e custodire le proprie password con la dovuta riservatezza (es. custodendole in un cassetto chiuso a chiave o su dispositivi cifrati);
- evitare di scrivere le proprie password su foglietti di carta o agende, a meno che tali supporti cartacei non vengano custoditi in cassetti o armadi chiusi a chiave;
- nel digitare sulla tastiera la password, prestare attenzione ad eventuali sguardi indiscreti;
- comunicare tempestivamente al responsabile di sistema eventuali dubbi sulla segretezza della password;
- cambiare immediatamente la password che sia stata comunicata a terzi o conosciuta da terzi, e ogni volta che ci sia il sospetto che non sia più segreta;
- modificare immediatamente la password nel caso sia stato necessario fornire le credenziali ai tecnici intervenuti per la manutenzione del computer o del software;
- evitare sempre di salvare la password sul browser, sull'applicazione, sulla posta elettronica, o quando proposto dal sistema operativo, per non doverla digitare all'accesso;
- non lasciare impostata la password di default fornita per l'accesso alle piattaforme IT.

- modificare la password temporanea assegnata dall'amministratore, al primo utilizzo (primo log-on);

Ufficio per la transizione al Digitale
Lungomare Nazario Sauro, 33 - 70123 Bari – tel. 080 540 3727 – 080 540 6918
resp.transizionedigitale@regione.puglia.it
resp.transizionedigitale@pec.rupar.puglia.it

Difendersi dal phishing

- non digitare le proprie credenziali su siti web raggiunti tramite link presenti in messaggi e-mail o altri documenti;
- nell'utilizzo della posta elettronica, evitare di aprire allegati che contengono un'estensione doppia o con estensione VBS, SHS, PIF, EXE, COM o BAT;
- se si ricevono e-mail non richieste o con contenuti pubblicitari, evitare di seguire i collegamenti a indirizzi Web eventualmente presenti nel testo delle e-mail;
- nel caso si riceva un messaggio di e-mail da una persona conosciuta, ma con un contenuto insolito, effettuare un controllo con il mittente prima di aprire l'eventuale allegato; infatti alcuni virus sono in grado di trasmettere messaggi con allegati che sembrano spediti da mittenti conosciuti;
- non inserire dati riservati riguardanti codici di carte di pagamento, chiavi di accesso al servizio home banking o altre informazioni personali richiesti tramite e-mail;
- diffidare di e-mail con indirizzi web molto lunghi, contenenti caratteri inusuali e scritti in modo non corretto;
- inoltrare al Presidio (informatica@regione.puglia.it) i messaggi che si ritengono sospetti per una valutazione prima di procedere con qualunque operazione, analogamente a quanto già previsto nel caso di segnalazioni di malfunzionamenti di problematiche informatiche;
- assicurarsi, al momento dell'inserimento dei dati riservati in una pagina web, che si tratti di una pagina protetta (riconoscibile in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con ''https://'' e non con ''http://'' e nella parte in basso a destra della pagina è presente un lucchetto).

GESTIONE DELLE POSTAZIONI DI LAVORO

Custodia della postazione di lavoro

- evitare di lasciare incustodito e accessibile il PC ed eventuali documenti durante una sessione di lavoro, soprattutto se comporta il trattamento di dati personali;
- impostare uno screen-saver con password o altro meccanismo di sicurezza per proteggere l'accesso alla propria postazione di lavoro nel caso di assenza anche temporanea;
- proteggere la postazione di lavoro utilizzando il blocco dello schermo (Su Windows attivazione rapida con la pressione contemporanea dei tasti + L), password di qualità e screen saver (da attivare su richiesta o dopo un tempo prestabilito di inattività), nel caso in cui ci si assenti temporaneamente dall'ufficio/stanza;
- al termine delle attività sulla propria postazione di lavoro, effettuare sempre la procedura di arresto del sistema ed attendere che sia terminata prima di lasciare l'ufficio.

Prevenzione dei virus informatici

- tenere aggiornati i computer con gli aggiornamenti dei relativi sistemi operativi e dei software installati, laddove possibile (per alcune situazioni, esempio utilizzo di MIRWEB, è necessario mantenere alcune specifiche versioni di JAVA);

Ufficio per la transizione al Digitale
Lungomare Nazario Sauro, 33 - 70123 Bari – tel. 080 540 3727 – 080 540 6918
resp.transizionedigitale@regione.puglia.it
resp.transizionedigitale@pec.rupar.puglia.it

- assicurarsi che sia presente un antivirus aggiornato sulla propria postazione di lavoro (in caso contrario contattare immediatamente il Presidio per procedere con l'installazione);
- verificare il regolare funzionamento della procedura automatica di aggiornamento del programma antivirus, al fine di accertarsi che la procedura sia andata a buon fine;
- utilizzare il software rispettando le istruzioni del fornitore;
- non installare software non autorizzato sulla postazione di lavoro;
- verificare, tramite adeguato programma antivirus, i file, il software e i dispositivi di memorizzazione rimovibili (hard disk esterni, chiavette USB, ecc.) provenienti dall'esterno, prima del loro utilizzo;
- segnalare tempestivamente al Presidio (informatica@regione.puglia.it) qualsiasi presenza di virus sospetta che pregiudichi o abbia pregiudicato la sicurezza delle informazioni;
- nello scaricare dalla rete Internet programmi (es. software open source; freeware, shareware ecc.) e documenti (testi e tabelle che possono contenere dei "virus macro") necessari allo svolgimento della propria attività lavorativa, utilizzare unicamente i siti delle case produttrici dei medesimi o i link che esse stesse propongono sul loro sito;
- evitare di cliccare su icone dall'apparenza innocua che ricordano applicazioni associate ad immagini o musica, mostrate dagli allegati di posta elettronica in quanto possono nascondere "worm".

Si ricorda che tutte le segnalazioni devono essere inoltrate a *informatica@regione.puglia.it*

Ufficio per la transizione al Digitale
Lungomare Nazario Sauro, 33 - 70123 Bari – tel. 080 540 3727 – 080 540 6918
resp.transizionedigitale@regione.puglia.it
resp.transizionedigitale@pec.rupar.puglia.it