Mail di chiarimento inviata venerdì 4 marzo 2022

In questi giorni, il Garante Protezione Dati Personali si è nuovamente occupato di due tematiche importanti e quotidiane.
In primo luogo, essendo anche oggetto dell'attività ispettiva per il primo semestre del 2022, il Garante ha pubblicato un video informativo rivolto agli Utenti dei siti web, affinché siano sensibilizzati in merito a cosa "attendersi" nei contenuti dei siti stessi, sotto il profilo informativo in merito ai c.d. "**cookies**"
(area https://www.gpdp.it/web/guest/temi/cookie).

Nel video, che può essere visionato sulla pagina YouTube del Garante (link presente in calce), vengono evidenziati alcuni aspetti focali:
a) in caso di cookies "tecnici"
= è sufficiente dare solo informazione degli stessi sulla home page o nell'informativa
b) per altri cookies "non tecnici" occorre
1) che vi sia un *banner* a comparsa immediata di adeguate dimensioni
2) che il banner abbia un *comando* per *accettare* i cookie o altre tecniche
3) che il banner abbia un *comando* per *chiuderlo* senza prestare il consenso
4) che vi sia un *link* all'informativa completa
evidenzia altresì che la richiesta di consenso sul sito può essere riproposta in alcuni casi (ad es. se cambiano le condizioni di servizio o decorsi sei mesi dall'ultima richiesta), ma il consenso non può essere *presunto* (no allo "scrolling" della pagina come forma di consenso tacito), né *ritorsivo* (il cookie wall, realizza una forma di costrizione nell'esprimere il consenso per leggere i contenuti del sito).

Secondariamente, visto l'incrementarsi dell'allerta nazionale per i rischi da attacchi informatici, evidenzia ancora come sia necessario prestare attenzione alle tipologie di **phishing**, **spear phishing**, nonché a **malware** e ransomware, che possono colpire gli Enti della PA.

Per quanto riguarda il phishing (svolto sia mediante email, ma anche sms, social, telefonate, ..), come ricordato in precedenza si cerca di fare leva su alcuni dei meccanismi tradizionali: autorevolezza (fingersi un'Autorità), intimidazione (informare di potenziali conseguenze negative in caso di inazione), consenso sociale (agire per imitazione, conformandosi a quanto svolto da altri), penuria (indurre la percezione di un senso di penuria, fine scorte), urgenza (viene utilizzato un criterio di tempo limitato per rispondere), familarità (senso di familiarità o apprezzamento verso una determinata situazione).
In tal caso, si cerca di indurre in errore l'operatore all'apertura di un determinato documento o all'invio di determinate informazioni, attraverso un sistema di pesca a strascico.

Nello spear phishing, invece, si punta ad un bersaglio specifico ed individuato: il bersaglio puntato viene indotto all'errore mediante l'invio di comunicazioni (email, ma anche SMS o telefonate) direzionate e ben strutturate quanto a personalizzazione. L'operazione di attacco in questo caso è più sofisticata, ma punta, facendo leva magari su uno specifico lavoratore, ad ottenere l'accesso al sistema per poter poi svolgere attività illecite.

Uno dei suggerimenti svolti dall'Europol per controbilanciare questi fenomeni è quello di tenere sempre alto il livello di attenzione ed in caso di dubbi, prima di riscontrare email sospette o scaricare file, contattare il personale apicale oppure i consulenti ed il dpo.

Link alla pagina informativa sul phishing:
https://www.garanteprivacy.it/documents/10160/0/Phishing+attenzione+ai+pescatori+di+dati+personali.+Infografica.pdf/4786aabd-facb-4fe7-aecf-c529a4887253?version=5.0