

## Mese della cybersicurezza: i consigli di Aruba alla Generazione Z per difendersi dal rischio phishing

Lo scorso anno sono stati circa 10 milioni gli italiani che hanno subito violazioni digitali ed il 32% di questi apparteneva alla Generazione Z, in assoluto il target più colpito. Gli episodi, infatti, tendono a decrescere all'aumentare dell'età, colpendo il 31% dei Millennials (27-40 anni), il 22% della Generazione X (41-56 anni) e l'11% dei Baby Boomers (57-64 anni)<sup>1</sup>.

Come mai, dunque, i giovani tra i 16 e i 26 anni sono i più bersagliati? In parte perché le truffe online utilizzano in modo sempre più massivo gli strumenti digitali con cui questa generazione è cresciuta, dai social media ai servizi di instant messaging, in parte perché i criminali informatici prendono di mira target sempre più giovani, come ad esempio quello dei gamer: non è un caso, infatti, che ora che il gaming rappresenta una delle maggiori industry di entertainment al mondo, sia diventato uno tra i principali obiettivi del cybercrime.

Per questa ragione, **Aruba S.p.A.**, il principale cloud provider italiano leader nei servizi di data center, web hosting, e-mail, PEC e registrazione domini, ha deciso di avviare una campagna di sensibilizzazione indirizzata agli utenti della Generazione Z per aiutarli a riconoscere e difendersi da una delle più comuni truffe veicolate tramite internet: il phishing. Un'opportunità che si inserisce all'interno dello **European Cyber Security Month**, la campagna promossa dall'Unione Europea per tutto il mese di ottobre, al fine di promuovere tra i cittadini europei la conoscenza delle cyber minacce che colpiscono il web e delle soluzioni per contrastarle.

**Cos'è il phishing.** Si tratta di una truffa digitale, in cui si cerca di ingannare la vittima spingendola ad effettuare operazioni allo scopo di recuperare le sue informazioni personali come username, password o altri dati riservati. Generalmente, il criminale informatico invia false comunicazioni al soggetto, fingendosi un ente o un'azienda ben conosciuta o con cui è possibile siano già in corso conversazioni e relazioni, usando scuse plausibili per ottenere i dati personali della vittima.

Solitamente gli attacchi di phishing si presentano come comunicazioni digitali che giungono al destinatario via e-mail, via SMS (fenomeno noto come smishing), tramite un social network o sulle principali piattaforme di instant messaging e, generalmente, sono accomunati da una o più delle seguenti caratteristiche:

- comunicazione di una sospensione o blocco di un account senza alcuna spiegazione;
- sollecito di pagamento legato ad una determinata operazione entro una data di scadenza fittizia;
- presenza di un indirizzo web che include un dominio simile ma diverso da quello originale dell'ente;
- richiesta di informazioni private;
- errori ortografici nel corpo del messaggio.

Ma esistono una serie di accorgimenti che consentono ai ragazzi di navigare più sicuri e non cadere vittime dell'attacco, tra questi:

- **Controllare il reale mittente del messaggio.** Nonostante il mittente della comunicazione possa sembrare familiare, è sempre bene analizzare l'intestazione dell'email e controllare le informazioni aggiuntive relative a chi scrive. Le organizzazioni e gli enti scrivono sempre dal proprio dominio, bisogna dunque controllare che corrisponda a quello ufficiale.
- **Verificare se i link contenuti nel messaggio sono sicuri.** Molto spesso, nei messaggi di phishing sono presenti pulsanti che rimandano a pagine graficamente molto simili o uguali a quelle di aziende e servizi conosciuti dietro alle quali però si nasconde il responsabile dell'invio dell'email. Si tratta in realtà di pagine fittizie e l'inserimento dei dati nei campi richiesti è il metodo più utilizzato per rubare informazioni sensibili. Per verificare se l'indirizzo

<sup>1</sup> Fonte: Indagine Unipol-Ipsos, 2022

web a cui conduce un link è sicuro, è sufficiente avvicinare il puntatore del mouse al link stesso per controllare l'url, in basso alla sinistra del browser.

- **Esaminare se il messaggio è scritto in modo grossolano.** Nonostante i messaggi di phishing siano sempre più accurati nel contenuto e nella forma, molto spesso contengono errori grammaticali o sintattici che possono far insospettare le persone. Errori di ortografia, un cattivo italiano (o inglese) e un linguaggio estremamente semplice sono chiari indizi di una mail di phishing.

Nel dubbio, tuttavia, si può agire in due modi:

- **Controllare la propria area personale.** Soprattutto nel caso in cui il messaggio ricevuto sia relativo a pagamenti negati o rinnovo di servizi, prima di cliccare o eseguire le azioni richieste, è bene accedere alla propria area riservata relativa allo stato degli ordini o dei servizi a cui fa menzione il messaggio ricevuto. Se non sono presenti evidenze che possano aver giustificato l'invio del messaggio, si tratta probabilmente di phishing.
- **Verificare con il servizio clienti.** Se ancora non si è in grado di capire con certezza se si tratti di una frode o meno, è sempre meglio contattare il servizio clienti dell'azienda a cui l'email sospetta fa riferimento.

Se si è ormai caduti nel tranello, invece, ci sono una serie di operazioni da compiere per limitare i danni, tra queste:

- **Cambiare la password.** Nel caso siano state rivelate credenziali personali relative ai propri accessi su portali online, bisogna cambiare subito la password o chiudere direttamente il proprio profilo prima che gli hacker possano accedervi.
- **Contattare il servizio clienti.** Qualora l'account sia già stato compromesso e non sia più possibile fare il login con i propri dati, è necessario chiamare il servizio clienti per ripristinare manualmente i propri dati d'accesso.
- **Avvisare le aziende o gli enti colpiti.** Oltre al recupero dei propri dati personali, è opportuno segnalare l'attacco phishing ai soggetti che ne sono stati colpiti, così da poter prendere provvedimenti e intervenire tempestivamente per fermare la truffa.

In conclusione, è sempre più importante che tutti siano consapevoli dei rischi derivanti dalla rete, ma in particolare è essenziale sensibilizzare la Generazione Z, quella dei nativi digitali. Il fatto di essere i più pratici nei confronti degli strumenti che internet mette a disposizione non basta a proteggerli, anzi potrebbe indurli ad essere meno attenti rispetto alle precauzioni da mettere in atto per difendere la propria vita virtuale.

La familiarità che i giovani hanno con i social e il web, d'altronde, potrebbe diventare un'esca, in quanto chi trascorre molto tempo online ha più probabilità di essere preso di mira. È essenziale quindi educare i più giovani invitandoli a stare sempre attenti a dove e con chi condividono informazioni personali online, considerando che fenomeni come phishing, sextortion o cyberbullismo vengono puniti dalla legge e, quando ne si è vittime, è necessario denunciare alle autorità competenti senza timore.

Per saperne di più: <http://aru.ba/sicurezzatruffeonline>

Scarica l'infografica completa: <http://aru.ba/phishinginbreve>

**#CyberSecMonth**

## **Aruba S.p.A.**

*Aruba S.p.A. è contro la guerra.* Fondata nel 1994, è il principale cloud provider italiano e prima azienda in Italia per i servizi di data center, cloud, hosting, trust services, e-mail, PEC e registrazione domini, rivolti a privati, professionisti, imprese e Pubblica Amministrazione. Aruba gestisce 2,6 milioni di domini registrati, 9,4 milioni di caselle e-mail, 8 milioni di caselle PEC, 130.000 server gestiti, per un totale di 16 milioni di utenti. Aruba PEC e Actalis sono le 2 Certification Authority di Aruba, entrambe accreditate presso AgID (Agenzia per l'Italia Digitale), erogano servizi altamente qualificati. A marzo 2021 Aruba entra nel mercato Telco con l'offerta di servizi di connettività ultra-broadband nel territorio italiano, basati sulla rete interamente in fibra ottica (FTTH - Fiber To The Home) di Open Fiber. In quasi 30 anni l'azienda ha acquisito lunga esperienza nello sviluppo e nella gestione di Data Center ad alta tecnologia, di proprietà, e collocati sul territorio nazionale (il più grande è a Ponte San Pietro - BG), caratterizzati da infrastrutture e impianti 'green by design'

conformi ai massimi standard di sicurezza del settore (Rating 4 ANSI/TIA-942) e progettati per avere il minimo impatto ambientale. Dal 2015 l'azienda soddisfa interamente il proprio fabbisogno complessivo con energia proveniente al 100% da fonti rinnovabili e produce anche la propria energia attraverso impianti fotovoltaici, sistemi geotermici e centrali idroelettriche, tutti di proprietà. Il network delle infrastrutture si estende anche in Europa con un Data Center proprietario in Repubblica Ceca e strutture partner situate in Francia, Germania, Polonia e UK. Dal 2014 Aruba è Registro ufficiale dell'autorevole estensione '.cloud' per la registrazione in tutto il mondo dei domini Internet. Dal 2015 Aruba.it Racing è team ufficiale Ducati nel Campionato Mondiale Superbike. Per ulteriori informazioni sul Gruppo Aruba visitare il sito: <https://www.aruba.it>

## Ufficio Stampa Aruba:

### **SEIGRADI**

*Barbara La Malfa / Stefano Turi*

Email: [aruba@seigradi.com](mailto:aruba@seigradi.com)

Sito: <https://www.seigradi.com/>

### **ARUBA S.p.A.**

Email: [ufficio.stampa@staff.aruba.it](mailto:ufficio.stampa@staff.aruba.it)

Sito: <https://www.aruba.it/>