

# Phishing: cos'è, come prevenirlo e come agire dopo un attacco

A cura di Nicola Tacconi, CISO di Aruba S.p.A.

Il phishing è una truffa veicolata tramite Internet, in cui si cerca di ingannare la vittima al fine di recuperare informazioni sensibili come username, password o dati bancari. Generalmente, il criminale informatico invia false comunicazioni al soggetto-vittima, fingendosi un Ente o un'azienda ben conosciuta o con cui è possibile che si stiano avendo conversazioni e relazioni, usando scuse plausibili per ottenere i dati personali della vittima. Il fenomeno del phishing è una minaccia attuale e frequente, tant'è che l'Italia, secondo una recente ricerca di Kaspersky Lab, è il quarto target mondiale di attacchi con il 5,76% di segnalazioni.

Secondo il [report 2019 di Clusit](#), l'associazione italiana per la sicurezza informatica, il phishing online non si è mai evoluto così velocemente come nell'ultimo anno, tanto che nell'arco del biennio 2017-2018 il numero di attacchi gravi è cresciuto in Italia del +37,7%. Solitamente il phishing si presenta come una comunicazione digitale che giunge al destinatario via e-mail, via SMS, tramite un social network o sulle principali piattaforme di Instant Messaging. Generalmente gli attacchi di phishing 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.

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

- **mantenere il proprio browser sempre aggiornato.** Installando le ultime versioni e inserendo dei filtri anti-spam, o degli appositi plug-in, il browser riuscirà a prevenire un maggior numero di tentativi di phishing;
- **controllare il dominio da cui proviene la comunicazione.** Una società o un ente scriveranno sempre dal proprio dominio, bisogna controllare che corrisponda a quello ufficiale. Questa verifica non dà la massima garanzia di autenticità ma rappresenta un primo controllo da poter effettuare;
- **fare attenzione a cliccare sui link nelle e-mail.** Come buona norma si consiglia di non cliccare mai sui link contenuti nella comunicazione ma digitare direttamente nel browser l'indirizzo del sito ufficiale del mittente della comunicazione e verificare sul sito il contenuto descritto nella comunicazione dell'e-mail;
- **utilizzare più indirizzi e-mail.** Quando ci si iscrive a servizi, o siti web, di dubbia affidabilità, è preferibile utilizzare e-mail secondarie, in modo da non rischiare di contaminare la propria casella e-mail principale;
- **contattare il servizio clienti.** Se arriva una e-mail ambigua e non si capisce con certezza se sia una frode o meno, è meglio contattare il servizio clienti dell'azienda a cui la mail fa riferimento.
- **segnalare un sito di phishing** aiutando altri utenti a non cadere nella truffa. Ogni segnalazione è utile per far comparire un messaggio di avviso riguardo al sito potenzialmente pericoloso: le segnalazioni possono essere inviate, ad esempio, tramite PhishTank, Google Safe Browsing o Microsoft Smart Screen.
- **utilizzare e-mail professionali**, dotate di protocolli di sicurezza quali [SPF](#) e DMARC sulla posta in ingresso (e in uscita).

Se, però, si è ormai caduti nel tranello, ci sono una serie di operazioni da compiere così da limitarne i danni, tra questi:

- **cambiare la password:** nel caso di portali online bisogna cambiare la password o chiudere direttamente il 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 contattare il servizio clienti per ripristinare manualmente i propri dati d'accesso;

- **contattare la banca.** In caso di furto di dati bancari va contattato l'istituto di credito per bloccare i servizi coinvolti nella truffa (carte di credito, conti correnti, bancomat ed ulteriori);

- **avvisare gli enti colpiti.** Oltre al recupero dei dati personali, è opportuno segnalare l'attacco phishing agli enti che ne sono stati colpiti, cosicché possano prendere provvedimenti e contrastare la truffa;

Il phishing, anche se può sembrare una semplice e-mail ingannevole, è un reato vero e proprio, e come tale va considerato. Motivo per cui il passo successivo alle eventuali segnalazioni è quello di informare le autorità competenti. Nonostante non sia previsto dall'ordinamento penale, il phishing oggi viene giudicato come frode informatica e furto d'identità digitale. In quanto reato informatico, inoltre, va comunicato alla Polizia Postale, che sul suo sito ha disposto uno spazio per le segnalazioni di questo tipo.

In conclusione, esiste una grossa mole di attacchi, ma grazie alle possibili contromisure da adottare, la percentuale di attacchi intercettati, bloccati e non andati a buon fine supera l'80%. Sul restante 20% è necessaria una consapevole collaborazione fra i fornitori di servizi e i clienti: leggendo attentamente le e-mail che si ricevono, inserendo i propri dati solo su siti affidabili e evitando di aprire link sospetti, il phishing può essere evitato.

Per saperne di più rimandiamo a [aru.ba/articoliphishing](http://aru.ba/articoliphishing)

## Aruba S.p.A.

*Aruba S.p.A., fondata nel 1994, è la prima società in Italia per i servizi di data center, cloud, web hosting, e-mail, PEC e registrazione domini e possiede una grande esperienza nella realizzazione e gestione di data center, disponendo di un network attivo a livello europeo: oltre ai data center proprietari - 3 già attivi in Italia ed uno in arrivo entro il 2020, più un altro in Repubblica Ceca - ulteriori strutture partner sono in Francia, Germania, UK e Polonia. La società gestisce oltre 2,6 milioni di domini, più di 8,6 milioni di caselle e-mail, oltre 6 milioni di caselle PEC, oltre 130.000 server ed un totale di 5 milioni di clienti. E' attiva sui principali mercati europei quali Francia, Inghilterra e Germania e vanta la leadership in Repubblica Ceca e Slovacca ed una presenza consolidata in Polonia e Ungheria. In aggiunta ai servizi di web hosting, fornisce anche servizi di server dedicati, housing e colocation, servizi managed, firma digitale, conservazione sostitutiva e produzione di smart-card. Dal 2011 ha ampliato la sua offerta con servizi Cloud e nel 2014 è diventata Registro ufficiale della prestigiosa estensione ".cloud". I Data Center di Aruba sono in grado di ospitare oltre 200.000 server.*

Per ulteriori informazioni: <https://www.aruba.it>

### Contatti per la stampa:

#### SEIGRADI

Barbara La Malfa / Stefano Turi

Via Eustachi, 31 – 20129 Milano (MI)

Tel. +39.02.84560801

Fax +39.02.84560802

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

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

#### ARUBA S.p.A.

Ufficio Stampa

Via Orti Oricellari 8/D

50123 Firenze

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

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