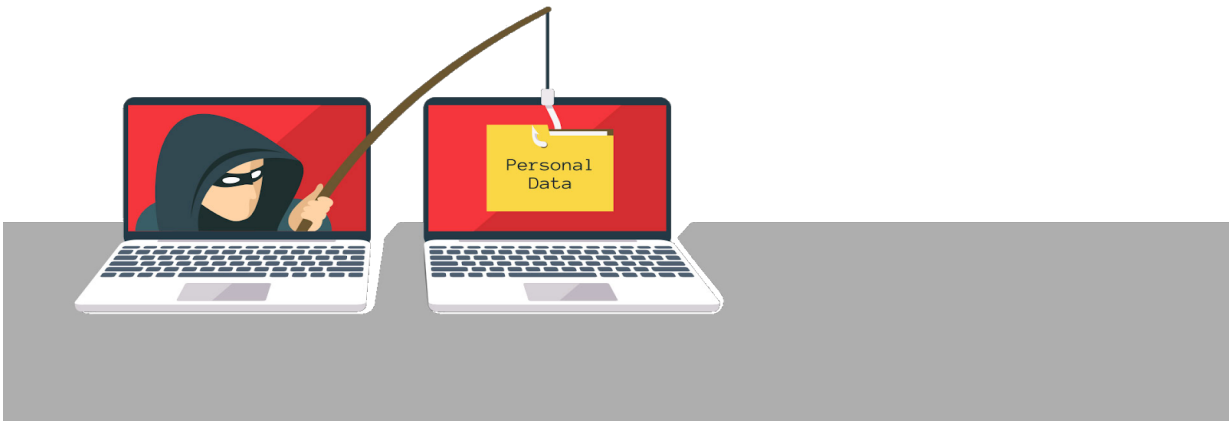
UNIVERSITÀ
DI SIENA
1240

UniSIcuri in Rete - ***Non abboccate al Phishing!***

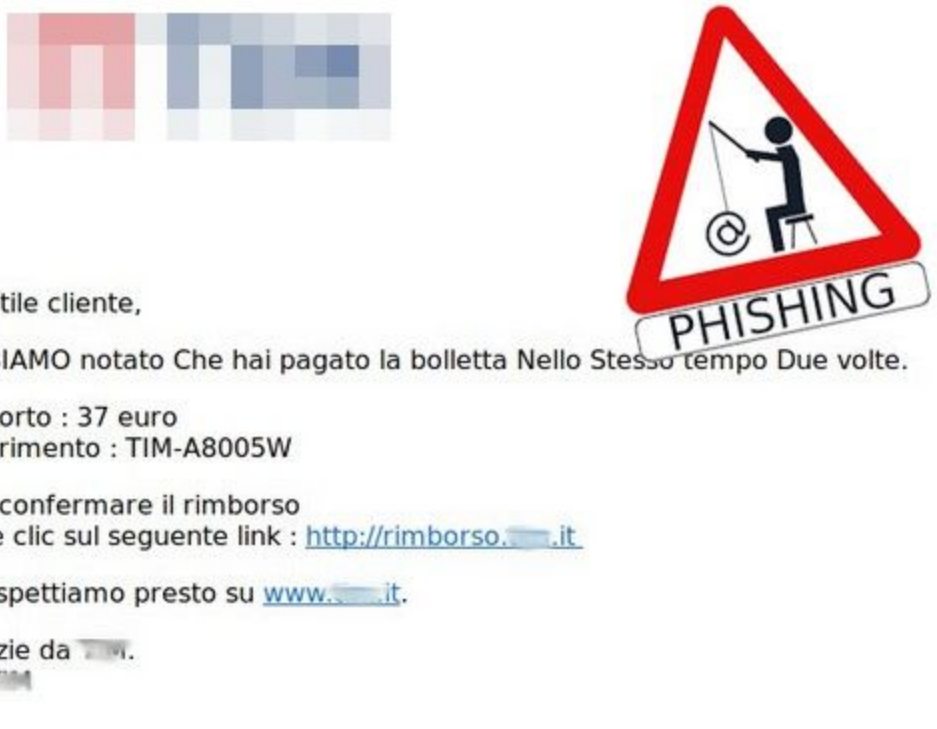
Novembre 2020



Non abboccate *al phishing!*

Ancora oggi, **il furto di credenziali attraverso sistemi di ingegneria sociale veicolati tramite e-mail** (il cosiddetto "*phishing*") rappresenta uno dei principali attacchi ai danni di privati, enti e aziende.

Spesso questi attacchi vengono condotti inviando **mail apparentemente legittime**, come provenienti da amministratori di sistema, da reparti contabilità o altro, chiedendo di cliccare su un link per autenticarsi o procedere con operazioni più o meno legittime.



Anche l'Università degli studi di Siena, in passato, è stata vittima di campagne di phishing indirizzate ai nostri utenti, tentando di ingannarli attraverso messaggi all'apparenza autentici, che però **nascondevano un tentativo di furto delle**

credenziali unisiPass: trovate alcuni esempi tra gli avvisi sulla pagina dedicata alla cybersecurity sul sito web dell'Ufficio esercizio e tecnologie.

👉 Il *phishing* fa leva sulle nostre paure, sfruttando tecniche di ingegneria sociale

---

Queste mail cercano di **indurre l'utente a cliccare su un certo link**, con le scuse più disparate come:

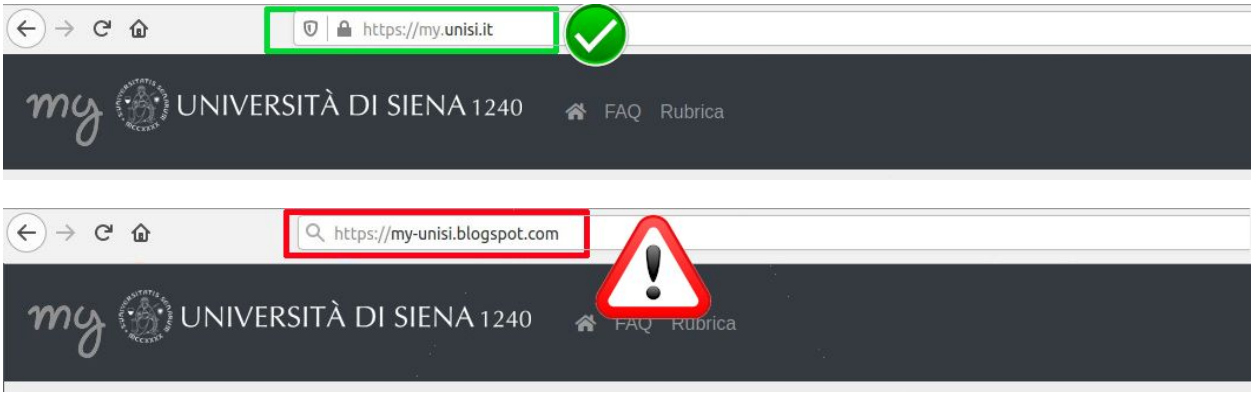
- la scadenza di una determinata password di un servizio online;
- l'accettazione dei cambiamenti delle condizioni contrattuali;
- il potenziale rinnovo della carta prepagata o della carta di credito;
- dei potenziali problemi inerenti accrediti, addebiti o trasferimenti di denaro su determinati conti online;
- la mancata, incompleta o errata presenza di informazioni, che magari riguardano determinati servizi bancari online;
- la presenza di offerte di lavoro particolarmente allettanti, che magari invitano ad inserire le coordinate bancarie per far sì di essere tra i primi a beneficiarne;

Potrebbe anche accadere che la mail provenga da un indirizzo che considerate autorevole, come ad esempio webmaster@unisi.it o similare: **ricordate che l'indirizzo del mittente può essere contraffatto con molta facilità** e non dovete sempre considerarlo un indicatore di autorevolezza.

È sempre necessario assicurarsi che la pagina web di destinazione sia attendibile e non farlocca, creata ad arte per rubare le vostre credenziali o i vostri dati: **verificare sempre che l'indirizzo sulla barra del browser sia corretto!**

👉 Un **indirizzo "non corretto"** è un indirizzo che non riconosciamo come simile agli indirizzi delle pagine e dei servizi che la email sostiene di riferire.

Nella figura seguente è riportato l'esempio di **un indirizzo valido di una pagina web della nostra Università** (https://my.unisi.it). Si notino sia la parte finale dell'indirizzo, che corrisponde all'insieme di indirizzi detenuti dall'Università di Siena e il protocollo *https* (soprattutto la 's' finale) che testimonia l'esistenza di un certificato che garantisce l'identità del server. Viceversa, l'indirizzo sottostante cerca di somigliare a uno plausibile ma **non appartiene alla famiglia degli indirizzi unisi.it**.



👉 Non fatevi ingannare da un aspetto grafico uguale a quello che già conoscete: fate le necessarie verifiche prima di inserire i vostri dati!

Ricapitolando, gli indicatori da considerare per identificare una mail di *phishing* sono:

- **contenuto dai toni perentori**, es. disattivazione di un servizio, perdita di soldi o di dati;
- **mittente non ufficiale o non conosciuto** (es. le mail dell'Università di Siena provengono da indirizzi @unisi.it);
- **il link dove viene richiesto di cliccare** non indirizza su una pagina o dominio ufficiale (es. *unisi.it*);

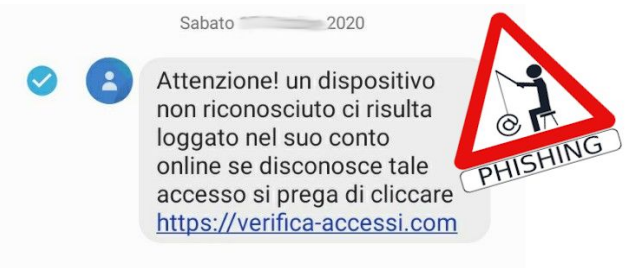
Potete esercitarvi nel riconoscere le mail fraudolente attraverso questo simpatico (e ben fatto) quiz messo a disposizione da Google: phishingquiz.withgoogle.com

Nel malaugurato caso foste caduti vittime di *phishing*, dovete procedere immediatamente al cambio di tutte le credenziali di autenticazione e monitorare attentamente tutti i movimenti bancari e/o accessi sospetti ai servizi utilizzati (denunciando, se necessario, alle autorità). Se sono coinvolte credenziali o dati dell'Università di Siena, dovete anche segnalarlo - *nel più breve tempo possibile* - all'indirizzo mail abuse@unisi.it.

Ricordiamo che **il servizio di assistenza tecnica Helpdesk (helpdesk@unisi.it) è a vostra disposizione** per aiutarvi a verificare l'autorevolezza di un messaggio di posta elettronica sospetto.

👉 Tra le contromisure implementate, segnaliamo l'adozione del feed di **OpenPhish.com** per bloccare l'accesso dalla Rete di Ateneo ai siti di *phishing* noti.

Attenzione che **il *phishing* non arriva solo attraverso le e-mail**: ultimamente sta aumentando il fenomeno dello *smishing*, ovvero ***phishing* via SMS**. I link malevoli arrivano via SMS direttamente sul vostro smartphone, invitandovi a cliccare per ritirare un premio, verificare un pagamento o una spedizione, etc etc etc...



👉 L'**87% degli attacchi di *phishing* sui dispositivi mobili** utilizza sms, app di giochi, messaggistica e social media

Nell'occasione, **comunichiamo che le mail relative alla scadenza delle credenziali di autenticazione *unisiPass*** hanno come mittente "*Helpdesk Università degli Studi di Siena <noreply@unisi.it>*" e il seguente layout:

UNIVERSITÀ DI SIENA 1240

Gentile ,

la password per l'account @unisi.it non viene aggiornata da **giorni**: per ottemperare a quanto previsto nella Circolare rep. n. 14/2019, prot. n. 40718 Gestione delle credenziali di autenticazione per i servizi informatici dell'Ateneo, è necessario procedere quanto prima al cambiamento della stessa.

Per **procedere al cambiamento della password**, può visitare il portale my.unisi.it e seguire le istruzioni indicate nella funzione "Modifica password":

PROCEDURA DI CAMBIO PASSWORD

ATTENZIONE: In caso di mancato aggiornamento entro il , l'account sarà bloccato.

Il pulsante "**PROCEDURA DI CAMBIO PASSWORD**" redirige alla pagina web https://my.unisi.it/password-change: verificate sempre, prima di inserire le vostre credenziali unisiPass, che l'URL sia affidabile.

Riferimenti

La normativa europea sulla protezione dei dati personali ("GDPR") impone la definizione di contromisure atte a minimizzare la possibilità del furto di dati ("*data breach*") e le eventuali conseguenze.

La rete Internet è diventata strumento indispensabile per l'espletamento di gran parte delle attività lavorative dell'Ateneo. Attraverso la Rete, l'Ateneo permette agli studenti, ai docenti, ai ricercatori, ai tecnici, agli amministrativi, ai collaboratori e a tutto il restante personale, l'accesso ai dati e ai servizi necessari allo svolgimento delle attività didattiche e amministrative. La sicurezza dei dati e delle infrastrutture assume, pertanto, un ruolo essenziale per le libertà e i diritti degli interessati e per il mantenimento della *business continuity*.

Qualsiasi dispositivo connesso in Rete diventa attore del processo di business e deve rispettare alcuni requisiti minimi per la salvaguardia dell'infrastruttura ICT e dei suoi servizi.

- ➔ **Garante per la protezione dei dati personali** - Regolamento europeo in materia di protezione dei dati personali - www.garanteprivacy.it/regolamentoue
- ➔ **Agenzia per l'Italia Digitale** - Glossario - *phishing* - cert-agid.gov.it/glossario/phishing/
- ➔ **Garante per la protezione dei dati personali** interviene sul *phishing* - www.garanteprivacy.it/temi/cybersecurity/phishing

Contatti e siti web utili

- ➔ Gestione delle **credenziali unisiPass** e **aggiornamento password**: my.unisi.it
- ➔ **Avvisi di sicurezza** dell'Università di Siena: www.uet.unisi.it/category/sicurezza/
- ➔ Servizio di **assistenza tecnica** Università degli Studi di Siena: helpdesk@unisi.it