Attività di phishing per impadronirsi delle credenziali di accesso ai servizi di Ateneo

Nel blocco "avvisi di sicurezza" troverete gli avvisi sempre aggiornati

Per Approfondimenti:

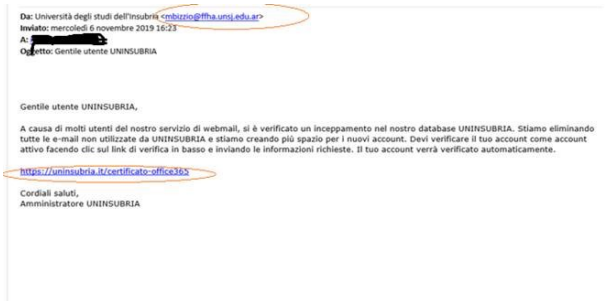
- Pratiche di cybersecurity di base per i dipendenti delle P.A.
- Phishing cos'è e come evitarlo

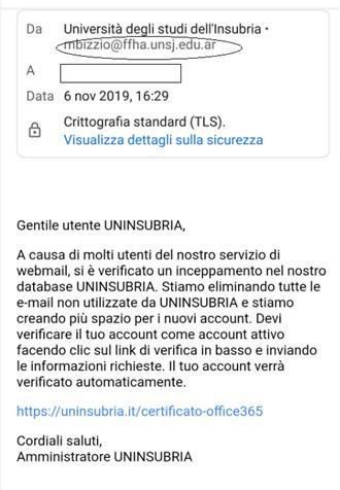
Email di Phishing per impadronirsi delle credenziali di accesso ai servizi di Ateneo

Aggregazione dei criteri
Gentili Utenti,

vi segnaliamo che in questi giorni è in atto una massiva campagna di *phishing* nei confronti di caselle di posta dell'Ateneo realizzato attraverso l'invio di messaggi che, come gli esempi che riportiamo in calce, richiamano i servizi di posta elettronica.

Vi invitiamo a prestare la **massima attenzione** e, soprattutto ad **eliminare** tali messaggi **senza cliccare su nessuno dei link in esso contenuti** (che, come potete vedere non sono collegamenti riconducibili a servizi di Ateneo) **e senza fornire le vostre credenziali** di accesso al servizio di posta elettronica.





Tali messaggi email sono ovviamente fasulli, e i relativi allegati **non devono essere assolutamente aperti**.

Nel caso che ciò inavvertitamente fosse avvento vi invitiamo a contattare **immediatamente** i referenti informatici di dipartimento e, per gli utenti dell'Amministrazione Centrale, il servizio di assistenza tecnica attraverso uno dei seguenti canali:

- *email:* **assistenza.tecnica@uninsubria.it**

- *portale web:* **https://ati.uninsubria.it/richiedi-assistenza**

- t*elefono*: **031 238 9779** oppure **0332 21 9779**

Per maggiori dettagli invitiamo a prendere visione all'avviso diramato dal servizio CERT della Pubblica Amministrazione:

https://www.cert-pa.it/notizie/messaggio-vocale-campagna-di-phishing-ai-danni-di-utenti-office-365/