UNIVERSITÀ
DEGLI STUDI
DI TORINO

A partire dal mese di luglio in tutte le sedi dell'Ateneo torinese saranno trasmessi dei video per sensibilizzare la comunità accademica sul tema dei reati informatici

Torino, 28 giugno 2024 - Anche a Torino il furto d'identità digitale è un reato sempre più diffuso, come conseguenza della maggiore presenza dei servizi informatici nella vita quotidiana e dell'uso diffuso delle tecnologie. Per questo motivo, gli utenti sono inevitabilmente esposti al rischio di sottrazione dei propri dati personali.

Le conseguenze del furto vanno dallo sfruttamento economico illecito delle informazioni all'uso dell'identità per fini penalmente illeciti: si pensi ai casi in cui il nome della vittima viene utilizzato per l'attivazione di finanziamenti, di servizi a pagamento, compravendite illecite o di adescamenti di minori in rete.

Il punto di partenza, nella maggior parte dei casi, è la sottrazione di documenti di identità del cittadino insieme alle credenziali di accesso alle piattaforme, anche tramite il ricorso a tecniche di phishing, social

engineering e spoofing (falsificazione dell’identità).

Per prevenire tali reati, la Polizia Postale e l’Università di Torino, grazie al protocollo d’intesa che li lega, a partire dal mese di luglio diffonderanno attraverso gli schermi pubblici presenti in tutte le sedi dell’Ateneo torinese alcuni video di sensibilizzazione sul tema. Messaggi brevi ed efficaci che informeranno studenti, docenti e personale tecnico di UniTo su come prevenire le nuove insidie digitali, utilizzando in modo più sicuro gli strumenti informatici nel quotidiano.

Nell’iniziativa di prevenzione sono trattate altre tematiche attuali come il rischio di incappare in truffe legate al falso trading online, che, dietro la prospettiva di facili guadagni, porta l’investitore a una perdita del capitale investito, o come il phishing, sempre più diffuso.

La Polizia Postale consiglia sempre di:

- non rivelare mai informazioni personali a sconosciuti o su canali non sicuri;
- non fornire nelle chat i propri dati personali;
- scegliere password sicure e differenziate per ogni singolo account;
- configurare sul proprio dispositivo sistemi di sicurezza come l’autenticazione a doppio fattore;
- non aprire gli allegati ai messaggi di posta elettronica se non dopo averli esaminati con un antivirus;
- diffidare da chi, spacciandosi per un operatore bancario o delle Forze dell’ordine, richiede di comunicare OTP o password;
- non lasciarsi ingannare da prospettive di guadagni immediati, diffidando tra l’altro dalle finte sponsorizzazioni ad opera di personaggi famosi, vittime a loro volta di sfruttamento indebito della propria immagine.