

VerbanoNews

Le news del Lago Maggiore

Riconoscere i segnali del catfishing: consigli per evitare frodi online

divisionebusiness · Tuesday, August 13th, 2024

Il catfishing rappresenta una minaccia sempre più diffusa sui siti di incontri online. Ad oggi, si tratta di una delle pericolosità più note e frequenti in assoluto, con decine di vittime ogni anno. Questo fenomeno, noto soprattutto per i suoi connotati di inganno e manipolazione, può mettere a rischio la sicurezza e la privacy degli utenti.

Proprio per questo motivo, diventa cruciale **essere coscienti del problema**, e saperlo analizzare alla radice, in maniera tale da avere qualche chance di individuarlo per tempo e anticipare l'arrivo dei problemi.

Questo fenomeno può infatti avere conseguenze molto gravi, sia emotive che finanziarie, per le vittime. Capire come identificare e prevenire il catfishing è fondamentale per navigare in modo sicuro nel vasto mondo delle relazioni virtuali.

Cos'è il catfishing e quali sono i pericoli

Per capire come difendersi da una qualsiasi minaccia, diventa importantissimo sapere di cosa si tratta.

Il **catfishing è una forma di truffa online** in cui un individuo crea un'identità falsa per ingannare gli altri. Questi truffatori possono adottare identità completamente inventate, o addirittura alterare la propria identità reale per scopi fraudolenti. Ci sono tantissimi casi, inoltre, in cui i catfish si fingono altri.

Hanno avuto una certa popolarità anche sui **siti di incontri occasionali**, ossia piattaforme di dating online pensate principalmente per utenti che non stanno cercando relazioni stabili, ma semplici incontri da una notte per un po' di divertimento. Siti specifici, con un'utenza ricca ed equilibrata.

Al di là di questo, comunque, i **pericoli associati al catfishing** sono molteplici e vanno ben oltre il semplice inganno emotivo.

Uno dei rischi principali del catfishing è la **perdita di controllo sulle proprie informazioni personali**. I truffatori mirano proprio ad ottenere dati sensibili delle persone, come numeri di conto bancario, informazioni di carta di credito o dettagli personali, che possono essere utilizzati per il furto di identità, minacce, truffe o altri fini illeciti. Il coinvolgimento emotivo in una relazione falsa può poi anche portare a danni psicologici significativi, soprattutto quando la truffa viene alla luce

dopo tanto tempo di frequentazione.

Come identificare un catfish

Come abbiamo detto precedentemente, uno dei rischi più potenti è proprio il coinvolgimento emotivo. In questo caso, **riconoscere un catfish può davvero risultare impensabile** quando le emozioni sono coinvolte a livello pesante.

Identificare un catfish **non è però impossibile**, anche se richiede attenzione e consapevolezza di alto livello.

Ci sono diversi **segnali** che possono indicare la presenza di un catfish online.

Uno dei segnali più comuni è la **mancanza di foto** o **l'uso di foto troppo perfette**, che sembrano provenire da modelli professionisti. I truffatori spesso cercano di mantenere l'anonimato per evitare di essere scoperti, e scegliere foto di modelli professionisti incrementa in maniera sbalorditiva il numero di persone che ci cascano.

Probabilmente, a volte la voglia di incontrare qualcuno di perfetto supera il razioicinio.

Altri segnali da tenere d'occhio includono **richieste di denaro o donazioni, racconti di situazioni difficili** che richiedono supporto finanziario e comportamenti generali sospetti, come la pressione eccessiva per condividere informazioni personali. Questi sono tutti campanelli d'allarme tipici di un catfish.

Se la persona con cui si sta interagendo evita costantemente di incontrarsi di persona, o di videochiamarsi, potrebbe essere un altro segnale importante.

La mente del truffatore: come ragiona

I truffatori di solito **agiscono con un piano ben definito** per manipolare le loro vittime.

Per raggiungere i loro obiettivi, spesso **giocano sulle emozioni** e sulle vulnerabilità delle persone, andando a toccare tasti emotivi che sanno di poter stimolare. Creano perciò **storie coinvolgenti e strappalacrime** per guadagnare fiducia e simpatia, spingendo così le persone a condividere informazioni personali sensibili anche senza pensarci.

Mantenere il mistero è una tattica comune per suscitare interesse e curiosità nella vittima.

Esempi di messaggi tipo del catfish

I **messaggi inviati dai catfish** possono seguire schemi ricorrenti che possono aiutare gli utenti a identificarli.

Questi messaggi spesso sono **eccessivamente dolci e lusinghieri**, cercano di creare un legame emotivo rapido o contengono errori grammaticali evidenti, che potrebbero indicare una provenienza geografica diversa da quella dichiarata.

Alcuni esempi comuni di messaggi di catfish includono **dichiarazioni d'amore precipitose**, richieste di denaro in situazioni di emergenza, o storie tragicomiche che cercano di suscitare compassione. Spesso, queste storie rasentano la follia, per cui diventa semplice identificarle.

Riconoscere questi schemi può essere la chiave.

Fact-Checking e come difendersi

Una delle strategie più efficaci per difendersi dal catfishing è praticare il **fact-checking**, ossia il processo di verifica delle informazioni per accertarne l'accuratezza e la veridicità

Verifica sempre le informazioni fornite dalla persona con cui stai interagendo, controllando la coerenza delle storie e cercando conferme esterne su ciò che ti dicono. Se qualcosa non torna o ti sembra sospetto, è meglio essere cauti e non condividere informazioni personali sensibili.

La propria privacy dev'essere il primo elemento da proteggere, sempre.

Non condividere mai informazioni come indirizzi, numeri di telefono, o dettagli finanziari con persone che non conosci bene. Se hai dubbi sulla veridicità di un profilo o di una persona online, è meglio interrompere immediatamente il contatto e segnalare il possibile catfish alle autorità competenti.

This entry was posted on Tuesday, August 13th, 2024 at 7:21 am and is filed under [Scienza e Tecnologia](#)

You can follow any responses to this entry through the [Comments \(RSS\)](#) feed. You can leave a response, or [trackback](#) from your own site.