

An abstract graphic on the left side of the slide, consisting of a network of white lines and small circles on a blue gradient background, resembling a circuit board or a neural network.

LA SICUREZZA IN RETE

LE REGOLE DA SEGUIRE PER LA SICUREZZA DELL'UTENTE ONLINE

1. Limitare e mantenere a un livello professionale le informazioni personali
2. Continuare ad usare le impostazioni sulla privacy
3. Navigare in maniera sicura
4. Assicurarsi che la connessione Internet sia sicura
5. Prestare attenzione a ciò che si scarica
6. Scegliere password complesse
7. Fare acquisti online da siti sicuri
8. Prestare attenzione a ciò che si posta
9. Prestare attenzione a chi si incontra online
10. Mantenere aggiornati il programma antivirus, il sistema operativo e le app.



CHE COS'È IL DARK WEB?



- Gli esperti considerano i termini *deep web* e *dark web* ingannevoli. Infatti, visitare il dark web non è di per sé illegale né implica effettuare azioni criminali. Servono solo strumenti adatti, i browser speciali, detti darknet, come TOR (che sta per The Onion Router), I2P e Freenet, che di fatto consentono la navigazione anonima.
- Secondo Nicolas Christin, professore alla Carnegie Mellon University, uno dei conoscitori più esperti sul tema, il dark web designa semplicemente tutte quelle pagine che non possono essere trovate dai motori di ricerca. E gran parte del deep web non ha niente di malevolo, viene, ad esempio, utilizzato da persone che vivono sotto regimi totalitari e non hanno libero accesso a Internet. Come dimostra il fatto che la BBC abbia creato una pagina sul dark web per consentire l'accesso a chiunque nel mondo.
- In una piccola parte del dark web sono però presenti i dark market, dei veri e propri portali e-commerce dove si trova di tutto: droghe, armi, killer, gioielli, film pedopornografici, dati trafugati, credenziali aziendali e bancarie...

CHE COS'E' IL DEEP WEB?

Il Deep web, nell'accezione italiana “web profondo” o “web sommerso” è l'insieme delle risorse presenti sul web che non sono indicizzate dai normali motori di ricerca. Ciò significa che l'attività degli utenti che operano all'interno del web sommerso è protetta dall'anonimato e non può essere analizzata



DIFFERENZE TRA DEEP WEB E DARK WEB

C'è una sottile differenza tra il deep web e il dark web.

- Mentre il deep web definisce i contenuti che sono su internet ma non vengono indicizzati (e quindi mostrati) dai comuni motori di ricerca come Google.
- Il dark web invece rappresenta l'insieme dei siti web, che offrono i loro contenuti attraverso un indirizzo IP nascosto (che non permette di individuare facilmente il proprietario del sito) e che sono accessibili soltanto attraverso la rete Onion, di cui parleremo più avanti.

COME ENTRARE NEL DARK WEB O DEEP WEB

- Lo strumento usato per entrare nel Dark Web è Tor (un acronimo che sta per The Onion Browser) progettato per assicurare l'anonimato sulle reti di computer.
- È necessario installare *Tor Browser* (disponibile per Windows, macOS, Linux e anche device mobile) che può essere utilizzato come un qualsiasi browser ma ha il vantaggio dell'anonimato.
- Una volta che si entra nel dark web con Tor si potrà navigare tra i vari siti, dei quali naturalmente si dovranno sapere gli indirizzi.

COSA SI TROVA NEL DARK WEB

- Armi, droga, gioielli, ma anche psicofarmaci, droga e carte di credito clonate erano ad esempio vendute su *Berlusconi market* (nessuna relazione con il politico italiano se non il nome) sgominato nel novembre 2019 e che rappresentava il quarto più grande sito di e-commerce illegale, dopo *Silk Road*, *Alpha Bay* e *Hansa Market*, tutti chiusi, ma probabilmente già rimpiazzati.
- Per ciascuna operazione si sa cosa è stato venduto, importo, modalità di consegna, prezzo in bitcoin.

QUALI SONO I PERICOLI DEL DARK WEB

- Il dark web è un luogo ideale per gli hacker per scambiarsi informazioni e virus in quanto è difficile risalire alle macchine da cui tali informazioni sono partite.
- È abitato anche da pirati informatici buoni che cercano di individuare e prevenire le minacce. Sicuramente la prospettiva di trarre vantaggi economici in un luogo oscuro è attraente per la criminalità. Questa per lo più vi cerca informazioni, dati personali, relativi ai conti bancari, password eccetera.

REATI INFORMATICI

FRODE INFORMATICA

La frode informatica viene definita come l'alterazione del funzionamento di un sistema informatico o telematico in grado di procurare a sé o ad altri un ingiusto profitto, un esempio è il phishing.



ACCESSO ABUSIVO A UN SISTEMA INFORMATICO O TELEMATICO

L'accesso abusivo a un sistema informatico o telematico protetto da misure di sicurezza, nonché il mantenimento in esso contro la volontà espressa di chi ne ha diritto. Per esempio l'accesso abusivo ai social network



DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI

Commette un reato informatico di questo tipo chiunque abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico, protetto da misure di sicurezza.



DIFFUSIONE DI PROGRAMMI DIRETTI A DANNO O INTERRUZIONE DI UN SISTEMA INFORMATICO

Chiunque diffonde, comunica o consegna un programma informatico da lui stesso creato per scopi di danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti, quindi l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.



INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE

Chiunque intercetta illegalmente le comunicazioni relative a un sistema informatico o telematico. Un esempio è il crimine informatico ai danni dell'utente finale è l'intercettazione dei dati di navigazione tramite la connessione a una rete Wi-Fi .

