Cybersecurity - Cap4 - Come proteggersi

1

00:00:05,160 --> 00:00:57,240

La prima misura di sicurezza, per così dire, che vi ho suggerito di adottare è quella di fare **attenzione a cosa pubblicate.**

Questo sembra banale ma invece è molto importante perché, se voi pubblicate tutto della vostra vita dovete prendere in considerazione o, meglio, dovete sapere che tutto ciò che pubblicate verrà visto da qualcuno e potrà essere utilizzato anche contro di voi.

Facciamo un esempio: se pubblicate la foto del vostro primo cane e magari scrivete sotto "Questo è il mio cane Spike" e poi, come domanda di sicurezza, quando perdete la password, avete "Come si chiama il tuo primo cane?" e avete messo "Spike" come risposta di sicurezza, capite che un hacker può entrare facilmente all'interno dei vostri account anche senza sapere la password.

2

00:00:57,240 --> 00:01:53,840

Questo è un piccolo esempio ma in realtà gli esempi sono moltissimi perché magari voi fate foto all'interno di casa e il ladro capisce se avete dei sistemi di sicurezza o no. Voi fate foto mentre siete al mare e il ladro capisce se siete o meno all'interno della casa; quindi, se la casa è libera oppure c'è qualcuno dentro e così via. Quindi capite che tutto ciò che pubblicate può avere delle conseguenze.

Io vi ho fatto degli esempi molto banali di qualcuno che semplicemente utilizza queste informazioni per entrare all'interno di un account, se non addirittura all'interno della vostra casa, ma gli esempi sono moltissimi. Quello che dovete ricordare sempre è che: **1. ciò che pubblicate può essere utilizzato da malintenzionati. 2. ciò che pubblicate resta sempre lì e incide sulla vostra vita**.

3

00:01:53,920 --> 00:04:03,200

Partendo appunto dalla prima casistica, quello che mi interessa evidenziare è che non si tratta di problemi che riguardano solamente gli sprovveduti, perché qualcuno potrebbe pensare "Ah sì, ma dai! Ma figurati se capiterà mai a me!"

No, non riguarda solo sprovveduti, riguarda tante persone. Ci sono anche giocatori dell'NBA, giocatori della nazionale di pallavolo italiana che subiscono quello che viene chiamato **lo "scam"**: vale a dire soggetti che ti contattano e ti fanno in qualche modo innamorare, sul lungo periodo, e poi ti chiedono dei soldi.

Ebbene, ci sono persone che hanno speso anche centinaia di migliaia di euro dietro a questi truffatori che si fingono magari una bella ragazza, un bel ragazzo, e fanno leva sul fatto che la vittima si è innamorata e poi chiedono i soldi. Guardate che queste sono truffe che davvero si verificano sempre più spesso e che riguardano sempre più spesso i giovani. Quindi fate molta attenzione agli amori online e quando qualcuno vi chiede soldi assolutamente diffidate. Non a caso, peraltro, sono stati creati anche dei programmi televisivi riguardo a questo tipo di situazioni, mi viene in mente "Catfish" che è uno di questi, che è proprio incentrato

sull' andare a scovare i truffatori che si fingono bei ragazzi, si fingono belle ragazze e, in realtà, sono semplicemente dei truffatori che hanno degli scopi secondari nei confronti della vittima.

Quindi fate attenzione a chi si interfaccia con voi, perché oltre al problema degli scam c'è anche **il problema dei pedofili**, purtroppo, dobbiamo ricordarlo, e quindi potrebbe esserci da parte qualcuno di più grande di voi, di molto più grande di voi, che potrebbe in qualche modo indurvi ad atteggiamenti sessuali e quindi fate attenzione a questo genere di situazioni.

4

00:04:03,360 --> 00:06:13,560

In particolare, ricordatevi una cosa molto importante che ha detto Guido Scorza e che a me piace ripetere spesso: **internet e i social network sono vietati a persone al di sotto di una certa età, solitamente 16,** per un motivo ben specifico, che non sono stati studiati per le persone più giovani.

Questa sembra una sciocchezza, ma non lo è. E l'esempio che fa Guido Scorza, e che io approvo totalmente, è questo: è come se prendiamo un ottovolante o roller coaster, una montagna russa, una giostra di un importante parco giochi e... magari quelli che fanno il giro della morte... Ok? Per capirci. E diciamo "Questa è stata progettata per persone che sono da un metro e 60 in su e quindi hanno, ad esempio, la sbarra che si chiude in maniera corretta e riesce quindi a evitare che le persone, nel momento in cui si fa il giro della morte, cada giù. Va bene? Seguitemi nel ragionamento!

Internet è come questa roller coaster e voi, se siete troppo piccoli e cercate di entrare nei social o in altri ambiti che non sono stati progettati per voi, è come se cercaste di salire su una montagna russa progettata per persone alte e magari siete ancora alti un metro. Al primo giro della morte, cadete e vi fate molto male.

Quindi pensate a questa metafora che, secondo me, si addice molto al mondo di internet e fate davvero attenzione e rispettate quelli che sono anche i termini di utilizzo. E anzi un appello che posso fare in questo momento è di sensibilizzare anche i vostri genitori, fatelo anche voi, dicendo di evitare di pubblicare vostre foto, vostri video... continuamente, perché quello potrebbe portarvi a conseguenze negative senza che neanche i vostri genitori o i vostri docenti abbiano preso in considerazione questo effetto malevolo.

5

00:06:13,640 --> 00:07:49,720

La seconda cosa che volevo dirvi, sempre su ciò che pubblicate sui **social network** in particolare, è che **quello che pubblicate rimane lì per sempre** e dovete sapere che i recruiter, magari adesso non vi interessa ma tra qualche anno sì, i recruiter sempre più spesso vanno a guardare qual è la vita social di una persona, la **"brand identity".** Si parla anche di questo "social identity", perché vanno a vedere nei vostri social network, nei vostri profili social. Magari vi chiedono l'amicizia e vanno a vedere chi siete, cosa fate... E, tendenzialmente, lo so perché ci sono passato anch'io, quando uno è un ragazzo tendenzialmente pubblica o dice cose che non pensa assolutamente magari qualche anno dopo, quando va a cercare lavoro, ma rimangono lì, perché nessuno va indietro a cancellare, almeno che non cancellate il profilo tout court, ma anche quello è un qualcosa che fanno in pochi. E quelle cose che avete fatto vengono viste dal recruiter, quindi da quello che potrebbe darvi il lavoro, e vengono giudicate da quello che potrebbe darvi il lavoro. E quindi magari, se siete stati poco inclusivi, questa cosa, in una situazione particolare, questa cosa potrebbe incidere sulla vostra possibilità di ambire ad un posto di lavoro.

Quindi fate molta attenzione a quello che pubblicate sui social network perché potrebbe incidere anche sulla vostra vita futura e sulla vostra vita lavorativa.

A tal riguardo avete mai sentito parlare di "social scoring"?

6

00:07:49,880 --> 00:10:19,920

Che cos'è il **social scoring**? "La cittadinanza a punti", qualcuno la chiama.

Ebbene, il social scoring è un sistema, che solitamente si serve di intelligenza artificiale, che punta a dare un voto ad ogni vostro comportamento e... attenzione, non si basa solo su ciò che è legale e ciò che è illegale ma semplicemente anche sui comportamenti virtuosi o meno virtuosi.

Faccio un esempio: se a scuola state andando bene/state andando male; avete un voto alto o basso in condotta; se siete più o meno simpatici... Ecco, è di questo che stiamo parlando, non stiamo parlando di violazioni o meno di leggi. Questo è molto importante definirlo in maniera netta. Ebbene, se tu hai un voto basso, uno scoring basso, in paesi come la Cina, ad esempio, non puoi accedere a determinate tipologie di istruzione; non puoi accedere a certe case; non puoi accedere a servizi come il treno o l'aereo...

Quindi capite che un qualcosa che è in grado di incidere, anche parecchio, sull'esistenza delle persone.

Ora, per fortuna, anche grazie all'intervento di molti attivisti a tutela della privacy, in Italia, questa cosa si sta diffondendo in maniera molto lenta. Per fortuna, ripeto. Tuttavia, qualora si dovesse espandere, qualora ci dovesse essere un via libera ufficiale anche al social scoring in Italia, questo potrebbe essere un grosso problema per chi, come dicevamo prima, ha deciso di pubblicare foto magari sconvenienti, oppure dei post con pensieri, con proprie idee, poco conformi. Anche per questo, attenzione, è importante far sì che ci si opponga....

È importante opporsi, in maniera netta, contro il social scoring, perché è giusto che chiunque abbia la possibilità di esprimere la propria opinione. Tuttavia, prevenire è meglio che curare, quindi, al fine di evitare di essere penalizzati nel caso in cui si diffondesse anche questa pratica in Italia... è sempre opportuno evitare di.. manifestazioni o comunque pubblicazioni poco convenienti sui social network.

7

00:10:20,000 --> 00:15:21,760

Sempre a proposito di social network, e della vostra vita sui social network, mi preme evidenziare una cosa molto importante: vi siete mai chiesti **come funzionano i social network?**

Vi siete mai chiesti come è possibile che, nel 2022, ci siano centinaia di migliaia di persone, in tutto il mondo, che pensano che la Terra sia piatta? Questa è una domanda che dovreste farvi.

Perché, se le persone sono state convinte di una cosa così evidente, che la Terra è piatta mentre non lo è, lo sappiamo tutti quanti, allora è possibile che i social network riescano ad incidere anche su aspetti meno evidenti e meno netti, come ad esempio orientamenti politici o decisioni, ad esempio, quelle che possono essere relative ad un referendum.

Facciamo un passo indietro prima di arrivare a questo output finale e cerchiamo di capire come funziona l'algoritmo dei social network.

Innanzitutto, ogni social network ha un proprio algoritmo, e questo è utile ricordarlo. Non sappiamo esattamente nel dettaglio come funzionano ma sappiamo con certezza che, in base alle vostre interazioni, l'algoritmo vi classifica... vi inserisce all'interno di un gruppo piuttosto che di un altro. E, banalizzando molto, facciamo questo esempio: voi entrate a quello che può essere, ad esempio, "Spotify"; nel momento in cui entrate per la prima volta e chiedete di sentire una canzone rap e Spotify, da quel momento, vi propone solo canzoni rap e più ne ascoltate, più vi propone. In quel momento diventa difficile anche solo pensare di "sprofilarsi" come qualcuno dice, vale a dire uscire da quel cluster, entrare in un altro cluster. Ma soprattutto, così facendo, non avrete mai la possibilità di scoprire cosa c'è al di fuori della vostra bolla: se domani uscisse il nuovo disco di un jazzista molto bravo o di una band rock, voi non potreste ascoltarla, perché Spotify, ma anche altri servizi simili... questo è importante ricordarlo, non è che stiamo puntando il dito, eh? **Vi propongono quello che è all'interno della vostra "bolla".**

La stessa cosa accade con i social network, perché tu entri per la prima volta in un social network e dici: "Mah, fammi vedere...solo per curiosità... che cosa dicono i terrapiattisti!"

Vai su un sito...su una pagina di terrapiattisti, ti informi ma non sei molto d'accordo.

Tuttavia, l'algoritmo ti registra come interessato a quel gruppo e quindi, da quel momento in poi, vedrai solo i tuoi amici che parlano di quello; solo news che parlano di quello; sono siti e pubblicità che parlano di quello.

A lungo andare, è molto probabile che questo ti convinca che quella è l'unica verità, perché non vedi altro!

E quindi questo, oltre a polarizzare le opinioni all'interno del dibattito pubblico, fa sì che le persone vengano in qualche modo convinte di cose che sono anche a volte assurde, come, ad esempio, che la Terra è piatta! Questo è un po' il ragionamento semplificato per spiegarvi che **il social network è in grado di** "clusterizzarvi" e quindi di profilarvi **ed incidere anche su quella che può essere la vostra percezione della realtà.**

Anche qui cito ancora una volta Guido Scorza del Garante della Privacy che, all'interno di una manifestazione, ha fatto questo esempio: se un tuo amico ti dice che una cosa è...ad esempio...che il cielo è fucsia... tu dici: "Mah...non credo che sia esattamente così!" Se te lo dicono in due, in tre...inizi un po' a dubitarne. Se tutti gli amici che hai attorno, tutte le news che hai attorno e tutte le pubblicità ti dicono che il cielo è fucsia, a lungo andare, tu credi che il cielo sia fucsia.

Quindi questo è un po' il meccanismo che sta dietro ai social network. È stato creato in realtà non con fini negativi ma con una finalità ben precisa: quella di permetterti di vedere solo cose che ti interessano. Ma, naturalmente, purtroppo, per forza di cose, il risvolto negativo è che, da lì in poi, non ti permette di vedere anche altre cose e quindi questo diventa un grosso problema perché, se utilizzato a proprio favore da malintenzionati, può portare anche a risultati assolutamente non auspicabili.

8

00:15:21,840 --> 00:16:18,760

L'inchiesta contro Cambridge Analytica ha difatti evidenziato la possibilità di incidere sulle elezioni e la probabilità che questo funzionamento degli algoritmi abbia inciso anche proprio sulla Brexit, causando un effetto dirompente che tutti ormai conosciamo. Quindi la vostra vita sui social e come vivete sui social ha degli effetti anche in questo senso.

E quindi, mi raccomando, anche quando navigate su TikTok Facebook, Instagram... a volte provate a guardare cose che magari non rientrano nella vostra bolla. **Cercate di "sprofilarvi",** come si suol dire, e quindi andate a curiosare qualcosa che magari pensate non vi interessi.

È probabile che riusciate a scoprire qualcosa di molto interessante e soprattutto è probabile che riusciate un po' a confondere l'algoritmo!

9

00:16:18,840 --> 00:18:24,560

Parliamo adesso di **antivirus.**

Parlare di antivirus al giorno d'oggi sembra quasi anacronistico, eppure, ancora oggi, quasi il 50% dei computer risulta non protetto da un antivirus.

L'antivirus è la prima barriera.

È molto importante perché, anche se è molto banale, riesce a bloccare quasi l'80% degli attacchi, quindi è assolutamente molto importante munirsi di un antivirus! Certo, se teniamo un antivirus di quelli particolarmente performanti è sempre meglio, ma esistono anche quelli gratuiti che a volte hanno delle performance di tutto rispetto. Quindi, piuttosto che niente... è meglio piuttosto, anche in questi casi! Quindi, se riuscite, prendete quello a pagamento, performante, sennò cercate in una versione gratuita, anch'essa performante, ma mi raccomando è molto importante che il device sia protetto da antivirus.

Attenzione, perché qualcuno a questo punto mi dice: "Ah, ma tanto io ho un sistema iOS, quindi Apple, e quindi non ho bisogno degli antivirus. Non è vero, è sbagliato perché anche i sistemi iOS hanno bisogno di sistemi di protezione che magari non riguardano i cosiddetti "virus.exe", perché il ".exe" non si può installare sul sistema iOS, ma riguardano altri tipi... altre tipologie di "malware", questa è la parola corretta da utilizzare e non "virus".

Quindi fate molta attenzione!

Fate molta attenzione anche ai vostri device portatili! Ebbene, noi possiamo prendere l'antivirus migliore che c'è in commercio ma, come abbiamo già detto prima, **il problema principale è l'errore umano.**

Difatti dovete sapere che solitamente i virus si introducono o, meglio, i malware si introducono all'interno dei nostri sistemi... per via di nostri comportamenti: si parla di "social engineering".

10

00:18:24,640 --> 00:21:23,400

Ecco, **il social engineering**... come avviene?

Avviene in due modalità.

O si inviano...invia un attacco a tappeto, quindi migliaia di e-mail vengono spedite istantaneamente a migliaia di indirizzi e qualcuno abbocca, **il cosiddetto phishing**, e qualcuno abbocca e mette dentro dei dati personali, la password, oppure clicca sul link che è sbagliato e che, in realtà, ti fa installare un malware.

Oppure ci sono situazioni in cui il social engineering avviene in maniera molto più accurata e quindi il malintenzionato che cosa fa? Si installa in qualche modo una backdoor all'interno del vostro sistema e vede le vostre interazioni, le studia in maniera dettagliata.

Studia anche come vi comportate, come vi parlate con un altro soggetto... e, ad un certo punto, quando ritiene il momento idoneo, assume le sembianze e, utilizzando lo stesso registro linguistico, cerca in qualche modo di estrapolare informazioni o addirittura denaro ad un soggetto terzo.

È successo davvero tante volte, quindi non pensate di essere esenti! Perché davvero quando uno pensa di essere esente, di essere al di sopra, è la volta buona che viene in qualche modo colpito! Ma è successo anche a persone davvero molto... di elevata caratura, di elevata esperienza.

C'è un noto imprenditore italiano che, di fatti, un giorno stava tenendo una convention e il proprio segretario, sapeva che non poteva disturbarlo, e riceve una e-mail da un collega o, meglio, da un presunto collega, che diceva:

"Guarda, mi devi fare questo bonifico di..." sparo una cifra... "di 1.000.000 euro."

Comunque era una cifra molto alta!

"E devi farlo subito."

Il segretario, sapendo che non poteva disturbare e comunque avendo visto che la mail arrivava dal collega appunto... o presunto tale... e che il registro linguistico era corretto.... e tutto quanto... ha fatto questo bonifico.

Ebbene, poco dopo si è scoperto che era un hacker che faceva finta di essere quell'altra persona, appunto al fine di ottenere questo pagamento.

Episodi come questi avvengono tutti i giorni e l'oggetto può essere il pagamento, ma anche una foto con contenuti espliciti, sessuali oppure credenziali o qualsiasi altra cosa. Quindi, mi raccomando, sappiate che ci sono questo tipo di situazioni e sappiate che è necessario in qualche modo fare attenzione ed evitare di trovarsi in queste situazioni.

11

00:21:23,480 --> 00:22:43,600

Dopo l'antivirus, l'altro grande pilastro della sicurezza di un sistema è **la password**. La password è un elemento davvero così banale che mai avrei pensato di dovermi trovare ancora, nel 2022, a ricordare alle persone di utilizzare password forti. In realtà ancora oggi, secondo fonti autorevoli, la password più utilizzata negli Stati Uniti è..."password"! La parola "password", scritta in maniera minuscola e lineare! Mentre in Italia la password più utilizzata è "123456"!

Quindi capite che, se utilizzate una password di questo tipo, è facilissimo per un hacker entrare all'interno dei vostri sistemi.

Considerate poi che oggi gli hacker non fanno più tutto a mano, hanno dietro degli algoritmi che studiano anche la vostra vita sui social... come dicevo prima...il vostro cane, i vostri parenti, tutto questo... e cercano di pensare a delle password e cercano in qualche modo di interagire anche col software per bucarlo, in qualche modo, e individuare quelle che sono le credenziali vostre corrette per entrare.

E quindi, attenzione, è molto importante introdurre delle password forti.

12

00:22:43,680 --> 00:29:11,280

I due errori principali che si fanno quando parliamo di password sono: utilizzare password deboli e l'altro è utilizzo della stessa password su più sistemi.

Quindi, noi possiamo utilizzare la password più forte del mondo, come si vede anche nel meme che avete nelle slide, ma nel momento in cui questa stessa password utilizziamo per più sistemi, per più social network, per più account e-mail e così via... diventa al pari di una password debole.

Perché?

Perché nel momento in cui ne buchi una, le buche tutte!

È successo più di una volta di trovarci in situazioni in cui un'azienda fornisce dettagli molto stringenti sulle password da inserire e poi quella password, pari pari, viene utilizzata anche per un social network. Nel momento in cui viene bucato il social network poi si va facilmente anche a bucare l'azienda che invece si era premurata di far utilizzare ai propri clienti una password molto forte.

Ma che cosa si intende quando si parla di **"password forte"?**

Solitamente, per tradizione e anche per best practices, le password forti sono quelle che hanno almeno otto caratteri e che hanno un numero al loro interno, hanno una maiuscola ed un carattere speciale.

Queste sono un po' le indicazioni base che vengono date però attenzione, perché il NIST, il National Institute della Sicurezza americana, ha precisato una cosa molto importante, ha detto: attenzione perché, se si utilizzano in sistemi di intelligenza artificiale, anche alcune password che magari formalmente rispettano questi limiti che abbiamo detto, queste indicazioni che abbiamo detto, sono facilmente bucabili, sono facilmente individuabili nei sistemi di intelligenza artificiale.

Faccio un esempio. Se noi scriviamo la parola "Pa$$word!" utilizzando la P maiuscola; al posto della S, il carattere speciale del dollaro e alla fine, dopo la D, un punto esclamativo… quella è una password che pur rispettando tutti i requisiti che abbiamo detto... magari forse non rispetta quello del numero delle cifre... Facciamo sempre un'ipotesi... che ci siano due punti esclamativi, e pur rispettando tutti i requisiti che abbiamo detto, è comunque debole perché l'intelligenza artificiale riesce a capire che quella cosa, anche con caratteri speciali, significa "password" e quindi, anche se abbiamo rispettato i requisiti, in realtà abbiamo creato un password sbagliata.

Quindi, anche per questo, il National Institute of Technology ci dice questo, ci dice: "Fate attenzione, non create comunque parole di senso compiuto utilizzando anche i caratteri speciali e cercate... mai... di non fermarvi alle otto cifre, ma di utilizzare tutti i campi possibili. Quindi se, ad esempio, una banca vi dà la possibilità di fare password di venti caratteri, fatele di venti caratteri!

Adesso ci sono quei sistemi, che ormai sono installati ovunque, che vi suggeriscono delle password e sono password assolutamente di senso non compiuto. Utilizzate quella e poi li andate a salvare su un sistema sicuro che è il cosiddetto "Wallet", e così siete a posto. Fondamentalmente sapete con certezza che la password è una password molto forte.

Se non dovesse bastare questo... e anzi solitamente non basta... il consiglio che vi diamo è di utilizzare, ove possibile, **l'autenticazione a due fattori**.

Forse non lo sapete, ma anche i social network hanno questa possibilità, vi forniscono questa possibilità. Questo significa che, ad esempio, se andiamo su Instagram possiamo attivare l'autenticazione a due fattori. In tal senso così se qualcuno vi ruba la password, prima di poter accedere, deve superare un'altra barriera.

Come funziona? Funziona così, che fondamentalmente bisogna dare a Instagram, in questo caso in particolare, un secondo contatto che può essere l'SMS oppure può essere l'Authenticator, che è un'app che è distribuita da vari distributori, da vari soggetti, e che ti permette di creare una seconda password parallela.

Ecco, nel momento in cui accedi da un device che non è il tuo solito, chiede la doppia autenticazione e quindi a quel punto la seconda autenticazione non va all'hacker ma va a te. E quindi tu sai innanzitutto che qualcuno sta accedendo, ma soprattutto è come se avessi una seconda porta che sbarra e impedisci l'accesso all'hacker.

Quindi, mi raccomando, essendoci questa possibilità, essendo anche gratuita e molto semplice, sfruttatela e utilizzatela, perché soprattutto fra i più giovani è molto ricorrente il furto delle credenziali, il furto dei profili social come Instagram, Tik Tok e così via.

Questo avviene anche perché c'è una diffusa moda, assolutamente da non seguire, che porta i ragazzi e le ragazze a fare una "prova d'amore": la prova d'amore dello scambio della password!

Sappiate che questa non è una prova d'amore, questa è solo una sciocchezza e se qualcuno vi dovesse chiedere "Scambiamoci la password, teniamo una password comune!"

Dite di no!

E se il vostro partner vi intima di fare questa cosa, se no vi lascia, significa che non è il partner giusto. Perché, come dicevo prima, ognuno ha diritto alla propria intimità e, soprattutto, chi oggi è il vostro partner, è il vostro migliore amico, domani potrebbe non esserlo. E quindi se oggi voi date la password alla persona sbagliata, e solitamente chi vi chiede la password è la persona sbagliata, questa potrà essere utilizzata contro di voi per diffondere materiale che magari non volevate diffondere.

Quindi diffidate da questo genere di situazioni, tenetevene alla larga e **abbiate cura della vostra password sicura.**

13

00:29:11,360 --> 00:30:38,200

Arriviamo quindi a uno dei discorsi cardine che si fanno quando parliamo di "mondo cyber", vale a dire il discorso del **cyberbullismo**.

Purtroppo il cyberbullismo è una piaga dei nostri tempi, un qualcosa che i ragazzi fanno anche magari con leggerezza, perché pensano che sia un reato senza vittime.

In realtà non è così.

Dovete sapere che il cyberbullismo ha vittime. E sono due in particolare le vittime, sono: chi pubblica e la vittima vera e propria del contenuto pubblicato.

Innanzitutto, che cos'è il cyberbullismo?

È la pubblicazione di contenuti che vanno in qualche modo a ridicolizzare o isolare un minore o la famiglia del minore.

Perché è importante parlarne?

Perché, al giorno d'oggi, soprattutto i ragazzi hanno accesso a molti... a molti canali e quindi è facilmente accessibile il canale ove inserire contenuti di questo tipo. Perché uno quando è giovane non ci pensa, pensa che sta facendo solamente uno scherzo, un qualcosa di divertente, un qualcosa che magari lo fa sentire anche forte rispetto alla propria comunità sociale, quindi al proprio gruppo di amici. Ma è un qualcosa che è un reato, è un illecito.

14

00:30:38,280 --> 00:32:35,640

E quindi innanzitutto mette chi pubblica sicuramente in una situazione difficile, che ha delle conseguenze anche su quello che è probabilmente il suo futuro, il futuro suo e della sua famiglia. Ma è un problema anche per la vittima che, nel caso migliore, è comunque la situazione peggiore, ma nel caso migliore si sente isolata e ha degli effetti drammatici a livello psicologico.

Ma nel caso peggiore può anche arrivare a gesti estremi: sono molti, infatti, i ragazzi e le ragazze che, a causa di cyberbullismo, negli anni, si sono magari tolti la vita o hanno fatto appunto gesti estremi.

Quindi assolutamente sconsigliato, perché è stupido e sciocco, pubblicare un qualcosa che va a denigrare un proprio compagno, un proprio amico o semplicemente un ragazzo o una ragazza di cui si hanno dei contenuti in qualche modo riconducibili al cyberbullismo.

Attenzione, perché la normativa della **legge n. 71 del 2017** si applica ai minori ma anche se fate qualcosa che riguarda, ad esempio, i vostri professori, perché purtroppo abbiamo visto anche questo, quindi atti di cyberbullismo nei confronti dei professori che vengono prima registrati, poi pubblicati magari su YouTube, sui social... Ecco, anche quel genere di cosa ha delle conseguenze, quindi ha delle conseguenze che incidono un po' meno sul maggiore di età, perché ormai si è formato... ha formato comunque una sua coscienza e quindi magari l'effetto psicologico è meno potente, ma sicuramente incidono sul bullo perché comunque la legge lo persegue e ha la possibilità di... in qualche modo punirlo.

15

00:32:35,640 --> 00:34:54,640

Una situazione molto simile si ha quando si parla di **"revenge porn".**

È simile ma ancor più grave perché, a quel punto, non parliamo semplicemente di bullizzare una persona ma di pubblicare contenuti, materiali altamente intimi.

Si parla di "revenge porn" perché ormai è quello il brand ma, in realtà, si dovrebbe parlare di **"pubblicazione di materiale intimo, non consensuale"**.

È un qualcosa che riguarda sia i minori sia gli adulti, questo... questa fattispecie è disciplinata **dall'articolo n. 144 bis del Codice della privacy.** E fate molta attenzione perché, oltre a rovinare delle vite, avrete sicuramente delle conseguenze di carattere legale. Quindi non fatelo mai, anche se la vostra ragazza o il vostro ragazzo vi ha fatto molto male, lasciandovi o tradendovi. Non è sicuramente questa la via da seguire per vendicarsi.

È molto importante parlarne, anche perché comunque ci sono dei modi per essere aiutati, perché se voi siete la vittima, e quindi voi non siete il bullo, avete la possibilità di parlarne con i vostri genitori, sicuramente; con i vostri docenti, sicuramente; ma anche col Garante Privacy.

Potete scrivere al **Garante Privacy.** Sono presenti già sul sito dei moduli molto facili da compilare e da inviare e il Garante Privacy, entro 48 ore, sia in caso di cyberbullismo sia in caso di revenge porn, ha la possibilità di intervenire e richiedere la cancellazione dei contenuti. E poi si procederà con la giustizia ordinaria per tutto il resto, per quelle che sono le conseguenze legali.

Quindi, mi raccomando, se siete la vittima sfruttate queste questi strumenti che vi mette a disposizione la normativa, l'ordinamento. Andate su un qualsiasi motore di ricerca, scrivete "Garante Privacy revenge porn"; "Garante Privacy e cyber bullismo"...scaricate il modulo e comunicate subito al Garante. Fatelo subito che in 48 ore riuscirete ad avere sicuramente un riscontro positivo.

Parlando di cyberbullismo e di revenge porn, non possiamo non parlare di un fenomeno che si sta sviluppando negli ultimi anni, vale a dire **il fenomeno del "Deep fake".**

16

00:34:54,640 --> 00:38:22,560

Che cos'è il deep fake?

È fondamentalmente un fotomontaggio molto avanzato che permette di sovrapporre l'immagine di una persona a quella che è invece la faccia di un'altra. Nelle slide avete degli esempi. Quella che vedete nella slide non è Ilary Blasi ma è un deep fake! Quella che vedete... Quello che vedete nella slide non è Tom Cruise ma è un deep fake! Quindi sono persone che vengono in qualche modo... a cui viene in qualche modo sovrapposta la faccia di un personaggio famoso e riescono in qualche modo ad assumerne le sembianze e a fare video che sembrano, in tutto e per tutto, originali.

Perché è importante parlarne?

Perché, al di là di quello che riguarda le persone famose, allo stato attuale, esistono tutta una serie di applicativi che ti permettono di fare questo genere di cose anche nei confronti di persone comuni, quindi anche nei miei confronti. E perché è importante? Perché, a volte, qualcuno potrebbe utilizzare questi sistemi in maniera malevola. Ad esempio, facendo video in cui una persona dichiara qualcosa di imbarazzante, oppure si spoglia, oppure facendo video che sfociano anche nel materiale sessuale.

Questo può rovinare le vite e può rientrare anche un concetto di cyberbullismo o di revenge porn, sotto certi aspetti. Si parla di "deep nude" anche in questo caso. Mi raccomando, anche in questo caso, se volete proprio utilizzare questi sistemi, utilizzateli, ma fatelo con senno e quindi non utilizzateli per denigrare le altre persone, i vostri compagni... Non utilizzateli assolutamente per creare materiale sessuale esplicito da divulgare online. Mi raccomando, questo è molto importante!

E attenzione, a tal riguardo, al fine di evitare di essere vittima di questo genere di situazioni, una delle cose che può essere d'aiuto è evitare di utilizzare in maniera troppo disinvolta o scusatemi... in maniera... cioè di evitare di utilizzare del tutto... applicativi come quelli che magari vi ringiovaniscono, vi invecchiano e vi fanno la versione maschile e la versione femminile...

Ecco, quelli in realtà non fanno altro che raccogliere tutte le informazioni del vostro viso, che poi potrebbero essere utilizzate proprio per questo genere di attività, perché è evidente che non basta una foto per creare un deep fake di voi, ma serve tutta la registrazione del reticolato che si basa un po' su quella che è la tecnologia di riconoscimento facciale e quindi servono anche molte foto che vanno a creare il reticolato corretto... che poi viene applicato e sovrapposto a quello della faccia dell'attore di turno.

Quindi evitate anche di scaricare quel genere di app perché non si capisce ancora benissimo che uso fanno delle vostre immagini e... A pensare male a volte si fa bene e quindi è possibile che quelle immagini vengano poi utilizzate anche contro di voi, anche semplicemente se un hacker va, buca i loro sistemi e pubblica quelle immagini. Come già è successo in alcuni sistemi di "proctoring" che utilizzavano, appunto, il riconoscimento facciale per verificare la correttezza dei compiti orali svolti a casa in periodo pandemico.

17

00:38:22,800 --> 00:40:50,200

Quindi fate attenzione, mi raccomando, e **non credete a tutto ciò che vedete!**

E siamo giunti quindi alla fine di questo percorso sulla cybersecurity.

Spero che vi sia piaciuto e spero di non avervi terrorizzato!

Spero di non avervi lasciato un ricordo negativo di quello che è l'ambito informatico, anche perché dovete sapere che non sono tutti hacker cattivi quelli che lavorano nella cybersecurity anzi, la cybersecurity e in generale il mondo tecnologico è un enorme opportunità per tutti voi e per tutti noi.

Perché?

Perché, come vedete anche nelle slide che vi sono state fornite, in realtà in Italia e nel mondo c'è un'enorme richiesta di professionisti per la cybersecurity. Professionisti che possono essere "pen tester", quindi quelli che fanno esattamente i "penetration test", che cercano di entrare nei sistemi evidenziando ciò che funziona e ciò che non funziona; professionisti che fanno i data analysis, che fanno le data analysis, scusatemi; professionisti che si occupano di consulenza; di intelligenza artificiale; di privacy...

Davvero, ci sono molte figure necessarie e molto utili e non credete totalmente a chi vi dice: "Ah, sarà sicuramente un futuro bruttissimo per tutti voi! Non avrete lavoro..."

Ma questo non è vero!

I lavori sono cambiati e ci sono, quindi basta semplicemente adattarsi alla realtà che sta mutando.

A tal riguardo voglio precisare solo una cosa: i professionisti che cercano nel mondo del lavoro non sono necessariamente degli informatici o degli ingegneri. No! Ci sono anche persone che hanno un percorso umanitario, quindi i filosofi. I filosofi oggi vengono utilizzati per riuscire a consultare e fare i cosiddetti "auditing etici" nei confronti dell'intelligenza artificiale. Ma anche gli avvocati, io stesso, per primo, lavoro nell'ambito del data protection.

Quindi mi raccomando, non lasciatevi scoraggiare da quelli che possono essere i pericoli del mondo tech.

Il mondo tech è sicuramente un'opportunità per tutti noi, basta saperla cogliere nel modo giusto!

Arrivederci!