“Ambasciatori della cultura della legalità”

Tema: Il cyberbullismo

In data 26/01/2017 la classe ha assistito al secondo incontro del progetto “Ambasciatori della cultura della legalità” concernente il bullismo e in particolare il cyberbullismo.

In primo luogo vorremmo chiarire la differenza tra bullismo e cyberbullismo. Un episodio di bullismo innanzitutto prende luogo in ambienti fisici come può essere quello scolastico, mentre la sua controparte virtuale richiede come prerequisito fondamentale non una zona appartata lontana dagli occhi di tutti, ma bensì una semplice connessione internet. Proprio ciò fa di questa belva una tra le più feroci in assoluto e per questo sono stati presi seri provvedimenti, come la campagna di sensibilizzazione che si svolge annualmente al Liceo scientifico A. Antonelli in cui vengono ricordati fatti come quello di Amanda Todd e disposte una serie di ammonizioni per usufruire del web in modo sicuro.
In questo mondo infatti la vittima è braccata 24 ore su 24 dove un così detto “leone da tastiera” ha come unico scopo quello di esibirsi su un palcoscenico virtuale per inveirle e innalzare il suo ego. Gli effetti però non si possono cancellare in questo caso, non sono semplici graffi o lividi, ma si tratta di ferite più profonde, più gravi, non rimarginabili. Il web in questi anni ci ha offerto un mondo di conoscenza e curiosità ma al contempo ha attuato una campagna di insensibilizzazione bombardandoci di video e immagini raccapriccianti, mostrandoci cose di cui avevamo soltanto sentito l’eco, abituandoci al pensiero che tutto ciò esiste al mondo ed è reale e quindi portando sempre più individui a cimentarsi in questi atti malsani data l’indifferenza comune. Questo concetto è stato toccato durante la conferenza tramite la visione di un video che grazie all’immagine struggente di una schiera di schermi luccicanti voltati verso un corpo inerme disteso in una pozza rossa ha dimostrato l’apatia a cui il genere umano sta andando incontro se continuerà a farsi controllare dal cyber-mondo. Questa parola non è stata scelta casualmente, ma bensì con il preciso scopo di mettere in guardia le generazioni future poiché il suo significato dal greco è “controllo” e in particolare allude all’arte di timonare una nave, quindi deve essere l’uomo in quanto razionale a usare e non essere usato.
In conclusione vorremmo focalizzare la nostra attenzione su un ultimo punto ossia: perché il cyberbullo agisce? Molte sono le opinioni ma il caso più generale è la voglia di essere notati, dettata probabilmente da una vita di solitudine. La semplicità del mezzo con il quale si compie l’azione, che garantisce quasi totalmente l’anonimato, e la già citata apatia diffusa forniscono il pretesto perfetto per chiunque per compiere un atto del genere. L’importante arrivati a questo punto è non banalizzare, non camminare a testa alta dopo aver compito un azione così tremenda con stampato in testa il motto “compiere azioni in qualsiasi momento per essere perdonati in qualsiasi momento” perché si creerebbe inequivocabilmente un mondo anarchico e appiattito, dove tutto ha lo stesso valore, da un suicidio a una nascita, perché questo segnerebbe la vittoria del cyber-mondo.

Il cyberbullismo è uno dei tanti pericoli diffusi sulla rete e anche uno dei più trattati perché interessa da vicino il mondo degli adolescenti e gli effetti ai quali può portare hanno spesso un impatto molto forte sulle persone.
Esistono però diverse minacce sul web che possono ledere sotto un punto di vista economico o intaccare in qualche modo la sfera privata di un soggetto. Anche se meno conosciute o più nascoste del cyberbullismo le pratiche come il phishing e il sexting alimentano un fenomeno ancora più grande che, celato ai nostri occhi, può avere delle conseguenze gravi nei confronti di una persona che può vedere distrutta la sua immagine sociale o comportare delle perdite ingenti di denaro.

Phishing

Il phishing è un tipo di truffa attraverso la quale un malintenzionato cerca di ottenere dalla vittima informazioni private o dati finanziari attraverso l’uso di Internet e dei suoi servizi o tramite le applicazioni di messaggistica online. Questa pratica utilizza una tecnica di ingegneria sociale che consiste nell’invio massivo di messaggi che imitano nell’aspetto e nel contenuto i messaggi legittimi dei fornitori di servizi. Attraverso questi messaggi i truffatori sono in grado di ottenere informazioni aziendali e personali come ad esempio il numero della carta di credito o la password per accedere ad un determinato servizio.

Tipologie

Esistono diverse tipologie o sottoinsiemi di phishing che vengono raggruppate in base alle diverse metodologie di truffa che utilizzano.

Spearphishing

Lo spearphishing è un attacco mirato verso un individuo o una compagnia. Gli attaccanti potrebbero cercare informazioni sull'obbiettivo per poter incrementare le probabilità di successo. Questa tecnica è, alla lunga, la più diffusa su internet, con una quota del 91% degli attacchi.

Clone phishing

È un tipo di phishing in cui una mail legittima viene modificata negli allegati o nei link e rimandata ai riceventi, dichiarando di essere una versione aggiornata. Le parti modificate della mail sono volte a ingannare il ricevente. Questo attacco sfrutta la fiducia che si ha nel riconoscere una mail precedentemente ricevuta.

Whaling

Di recente molti attacchi di phishing sono stati indirizzati verso figure di spicco e il termine whaling è stato coniato per questi tipi di attacco. Viene mascherata una mail/pagina web con lo scopo di ottenere delle credenziali di un manager. Il contenuto è creato su misura per l'obbiettivo è spesso scritto come un problema amministrativo o una lamentela di un cliente. Sono state utilizzate anche mail identiche a quelle dell'FBI cercando di forzare il ricevente a scaricare e installare del software.

Conseguenze

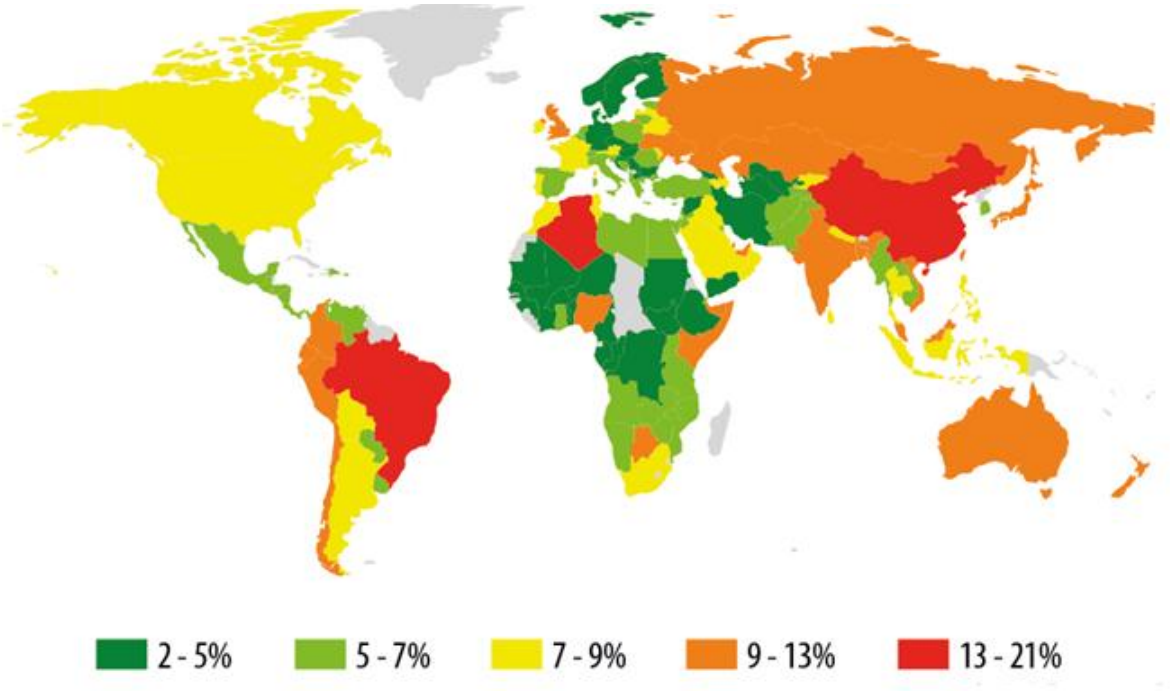
Le conseguenze di un attacco phishing su un soggetto posso essere:

- **Fisiche** se vi è una perdita indiretta di denaro come il blocco o il danneggiamento di un dispositivo elettronico dovuto all’installazione di un software maligno.
- **Economiche** se vi è una perdita diretta di denaro dovuto alla perdita di dati personali quali credenziali o dati di accesso finanziari.
- **Legali** se il proprio computer viene utilizzato per scopi illeciti.

Dati

C’è stata una notevole escalation di attacchi phishing nel 2016, secondo l’ultimo rapporto dell’**Anti-PhishingWorking Group** (**APWG**). Dai dati raccolti si nota quanto siano aumentati gli attacchi di phishing nel corso del primo trimestre di quest’anno, “rispetto a qualsiasi altro momento della storia”. C’è stato un enorme picco di attività di phishing tra ottobre 2015 e marzo 2016, con un incremento incredibile del **250%.**

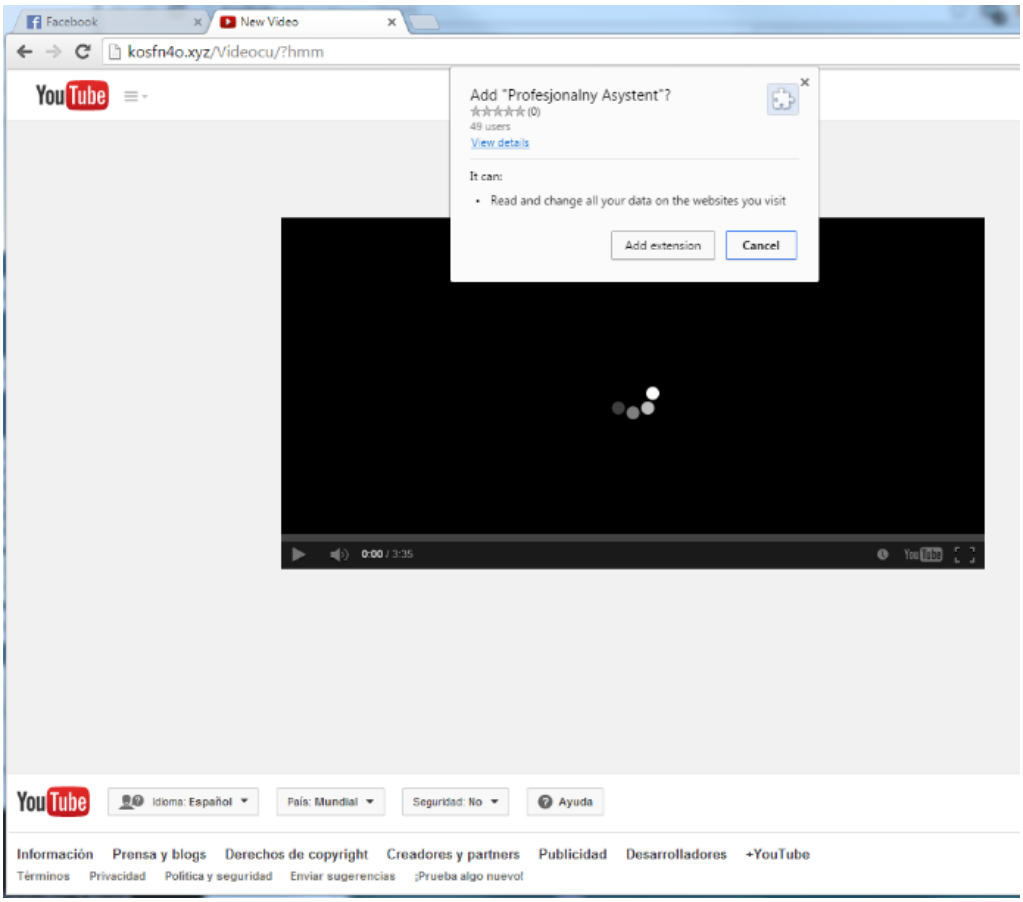
La geografia degli attacchi evidenzia che la quota percentuale più elevata di utenti sottoposti ad attacco da parte dei phisher è stata osservata in **Cina** (**20,22%**).



Ripartizione geografica degli attacchi di phishing – Situazione relativa al secondo trimestre del 2016

Esempio di phishing

Gli utenti di Facebook, il celebre social network, risultano spesso sottoposti ad attacchi orditi dai phisher. Nel corso di uno di tali assalti, verificatosi proprio nel secondo trimestre del 2016, i malintenzionati hanno preso di mira le potenziali vittime prospettando, per queste ultime, la possibilità di visualizzare un video “provocante”. Per far questo, gli utenti avrebbero dovuto recarsi su una pagina web fasulla, realizzata nello stile di YouTube, il popolare e frequentatissimo portale video, per poi installare un’apposita estensione per il browser.



Tale estensione avrebbe di fatto richiesto i diritti per poter leggere tutti i dati custoditi nel browser; potenzialmente, ciò avrebbe permesso ai malintenzionati di carpire, in seguito, password e login via via immessi dall’utente, nonché i dati sensibili relativi alle carte di credito utilizzate da quest’ultimo, ed altre informazioni di natura confidenziale appartenenti alla vittima.

Buone pratiche

IL BUON SENSO PRIMA DI TUTTO

Dati, codici di accesso e password personali **non** dovrebbero mai essere comunicati a sconosciuti. E’ bene ricordare che, in generale, banche, enti pubblici, aziende e grandi catene di vendita **non** richiedono informazioni personali attraverso e-mail, sms, social media o chat: quindi, meglio **evitare** di fornire dati personali, soprattutto di tipo bancario, attraverso tali canali. Se si ricevono messaggi sospetti, è bene **non** cliccare sui link in essi contenuti e **non** aprire eventuali allegati, che potrebbero contenere virus o programmi *trojanhorse* capaci di prendere il controllo di pc e smartphone.

OCCHIO AGLI INDIZI

I messaggi di phishing sono progettati per ingannare e spesso utilizzano imitazioni realistiche dei loghi o addirittura delle pagine web ufficiali di banche, aziende ed enti. Tuttavia, capita spesso che contengano anche **grossolani errori** grammaticali, di formattazione odi traduzione da altre lingue. E’ utile anche **prestare attenzione al mittente** o al suo indirizzo di **posta elettronica**. Meglio diffidare **dei messaggi con toni intimidatori**, che ad esempio contengono minacce di chiusura del conto bancario o di sanzioni se non si risponde immediatamente: possono essere subdole **strategie per spingere il destinatario a fornire informazioni personali**.

PROTEGGERSI MEGLIO

E’ utile installare e tenere aggiornato sul pc o sullo smartphone un programma **antivirus** che **protegga anche dal phishing**. Programmi e gestori **di posta elettronica** hanno spesso **sistemi di protezione** che indirizzano automaticamente nello **spam** la maggior parte dei messaggi di phishing: è bene controllare che siano attivati e verificarne le impostazioni. Meglio non **memorizzare dati personali e codici di accesso nei browser** utilizzati per navigare online**.** In ogni caso, è buona prassi **impostare password alfanumeriche complesse**, cambiandole spesso e scegliendo credenziali diverse per ogni servizio utilizzato.

ACQUISTI ONLINE IN SICUREZZA

Se si fanno acquisti online, è più prudente usare **carte di credito prepagate** o altri sistemi di pagamento che permettono di **evitare** la condivisione di dati del conto bancario o della carta di credito.

LA PRUDENZA NON E’ MAI TROPPA

Per proteggere conti bancari e carte di credito è bene **controllare spesso le movimentazioni** e attivare **sistemi di *alert*** automatico che avvisano l’utente di ogni operazione effettuata. Nel caso si abbia il dubbio di essere stati vittime di phishing è consigliabile **contattare direttamente** la banca o il gestore della carta di credito attraverso i **canali di comunicazione conosciuti e affidabili**.

Sexting

Il termine ***sexting***, deriva dalla fusione delle parole inglesi ***sex*** (sesso) e ***texting*** (inviare messaggi elettronici), è un neologismo utilizzato per indicare lo scambio di messaggi sessualmente espliciti e di **foto e video a sfondo sessuale**, spesso realizzate con il telefono cellulare, o nella pubblicazione tramite via telematica, attraverso canali come chat, social network, internet e varie app. Tali immagini, anche se inviate in origine a una ristretta cerchia di persone, in seguito si possono diffondere in modo incontrollabile e creare problemi seri alla persona ritratta.Questo fenomeno si presenta in grande percentuale tra 2 soli **partner** ma ci sono anche casi in cui l’invio di immagini avviene tra soggetti che non intrattengono alcun tipo di relazione.

Amanda Todd

Un noto caso di sexting è quello che coinvolge **Amanda Michelle Todd**, un'adolescente di 15 anni, che venne trovata senza vita nella sua casa di Port Coquitlam vicino a Vancouver il **10 ottobre 2012**.

Al secondo anno di scuola media, Amanda si divertiva a fare nuove conoscenze tramite una **video chat**. Durante una conversazione, alcuni amici chiesero alla ragazza di fotografarsi il seno. Dopo momenti di esitazioni alla fine cedette e si fotografò il seno nudo. Un anno dopo ricevette un messaggio nel quale il **ragazzo**, che era in possesso della foto sin dall'inizio, l'avrebbe **ricattata** minacciando di mostrare la sua foto in topless ai suoi amici, nel caso in cui lei non gli avesse mandato nuovamente qualche foto di nudo. Conosceva i suoi amici, l'indirizzo di casa, la sua scuola e persino i nomi dei suoi famigliari. All'alba del Natale successivo, la polizia bussò a casa sua alle 4:00 del mattino, informando la famiglia Todd che una foto di Amanda in topless stava circolando online. Amanda ne fu traumatizzata, manifestando **ansia**, **depressione acuta** e **attacchi di panico**. La sua famiglia cercò invano di aiutarla, trasferendosi. La ragazza iniziò a fare uso di **alcool** e **droghe**, con pesanti attacchi di ansia. Un anno dopo il **ricattatore** si fece nuovamente vivo: creò un falso profilo **Facebook** di Amanda, usando la sua fotografia in topless come foto profilo, facendo scoprire la vicenda ai nuovi compagni di classe, nella sua nuova scuola. Ancora una volta Amanda si trovò costretta a cambiare varie scuole e riallacciò i contatti con una sua vecchia conoscenza. Il **ragazzo** le propose di avere rapporti sessuali mentre la fidanzata si trovava in vacanza. Lei acconsentì, provava qualcosa per lui. La settimana successiva, lui, la sua ragazza e un gruppo di altri 15 ragazzi l'**aggredirono** all'uscita dalla scuola. Amanda tentò il **suicidio** ingerendo **candeggina**, ma si salvò grazie all'intervento tempestivo dei soccorsi. Al ritorno a casa Amanda lesse su Facebook **commenti offensivi** sul suo tentativo di suicidio. La sua famiglia si trasferì nuovamente in un'altra città, ancora senza risultati. Sei mesi più tardi ulteriori messaggi offensivi furono pubblicati sui social network. Il suo stato mentale peggiorò, trascinandola nella spirale dell'**autolesionismo**. Nonostante prendesse anti-depressivi e consultasse uno psicologo, ebbe un'overdose di medicinali e trascorse due giorni in ospedale. Amanda fu inoltre oggetto dello scherno di altri studenti nella sua scuola per i suoi **voti bassi**, conseguenza delle sue difficoltà di apprendimento e del tempo trascorso in ospedale per curare la sua depressione grave.

Il 7 settembre **2012**, Amanda Todd caricò su **YouTube** un video dal titolo *My Story: Struggling, bullying, suicide and self harm* (La mia storia: lotta, bullismo, suicidio e autolesionismo), nel quale, tramite una serie di **flashcard**, raccontava la sua esperienza. Al 30 settembre **2015** il suo video di denuncia aveva ricevuto oltre **11.823.419 visualizzazioni**, e il suo link fu presente in centinaia di siti web di testate giornalistiche di tutto il mondo.