Sicurezza e TIC

Prof. Pietro Prosperi

Sicurezza e TIC

Gestione e manutenzione di una LAN/WLAN, navigazione sicura, privacy, cyberbullismo, ecc.

CONTENUTI

Corso di gestione di una rete didattica

COMPETENZE

Acquisire conoscenze giuridiche e competenze tecniche necessarie per la gestione e la manutenzione di una rete didattica

SICUREZZA E TIC

- Gestione di una LAN/WLAN
- Sicurezza di un sistema distribuito
- Codice delle Privacy
- Policy di sicurezza
- Cyberbullismo

studio di Eurostat sulla sicurezza online

Ufficio statistico dell'Unione Europea

Relazione Eurostat in occasione del

Giornata per una rete più sicura

- Giornata internazionale di sensibilizzazione sui rischi di internet durante la quale si organizzano convegni e campagne su: cyberbullismo, pedopornografia e pedofilia on-line, al sexting, alla perdita di privacy e alla dipendenza da videogiochi
- Scopo : promuovere un uso responsabile della tecnologia e dei cellulari online, soprattutto tra i bambini e giovani

Relazione Eurostat

- Un quarto della popolazione europea ha riscontrato problemi di sicurezza in internet
- Conseguenza: utilizzo limitato del web per acquisti online, transazioni bancarie, connessioni wireless da luoghi diversi da casa
- Principali fonti dei problemi restano i virus
- Rischi:
  - perdita o diffusione di informazioni personali
  - perdite finanziarie
  - adescamento bambini

http://ec.europa.eu/eurostat/news/themes-in-the-spotlight/safer-internet-day

Gestione di una rete LAN/WLAN

PNSD - Accesso digitale

Azione #1 - Fibra per banda ultra-larga alla porta di ogni scuola: ogni scuola deve essere raggiunta da fibra ottica, o comunque da una connessione in banda larga o ultra-larga, sufficientemente veloce per permettere, ad esempio, l'uso di soluzioni cloud per la didattica e l'uso di contenuti di apprendimento multimediali;

Azione #2 - Cablaggio interno di tutti gli spazi delle scuole (LAN/W-Lan): le strutture interne alla scuola devono essere in grado di fornire, attraverso cablaggio LAN o wireless, un accesso diffuso, in ogni aula, laboratorio, corridoio e spazio comune;

Azione #3 - Canone di connettività: il diritto a Internet parte a scuola: per abilitare nuovi paradigmi organizzativi e didattici, e per fruire sistematicamente di servizi di accesso ad informazioni e contenuti digitali, ogni scuola deve poter acquistare la migliore connessione possibile.

Cos'è una rete LAN o WLAN

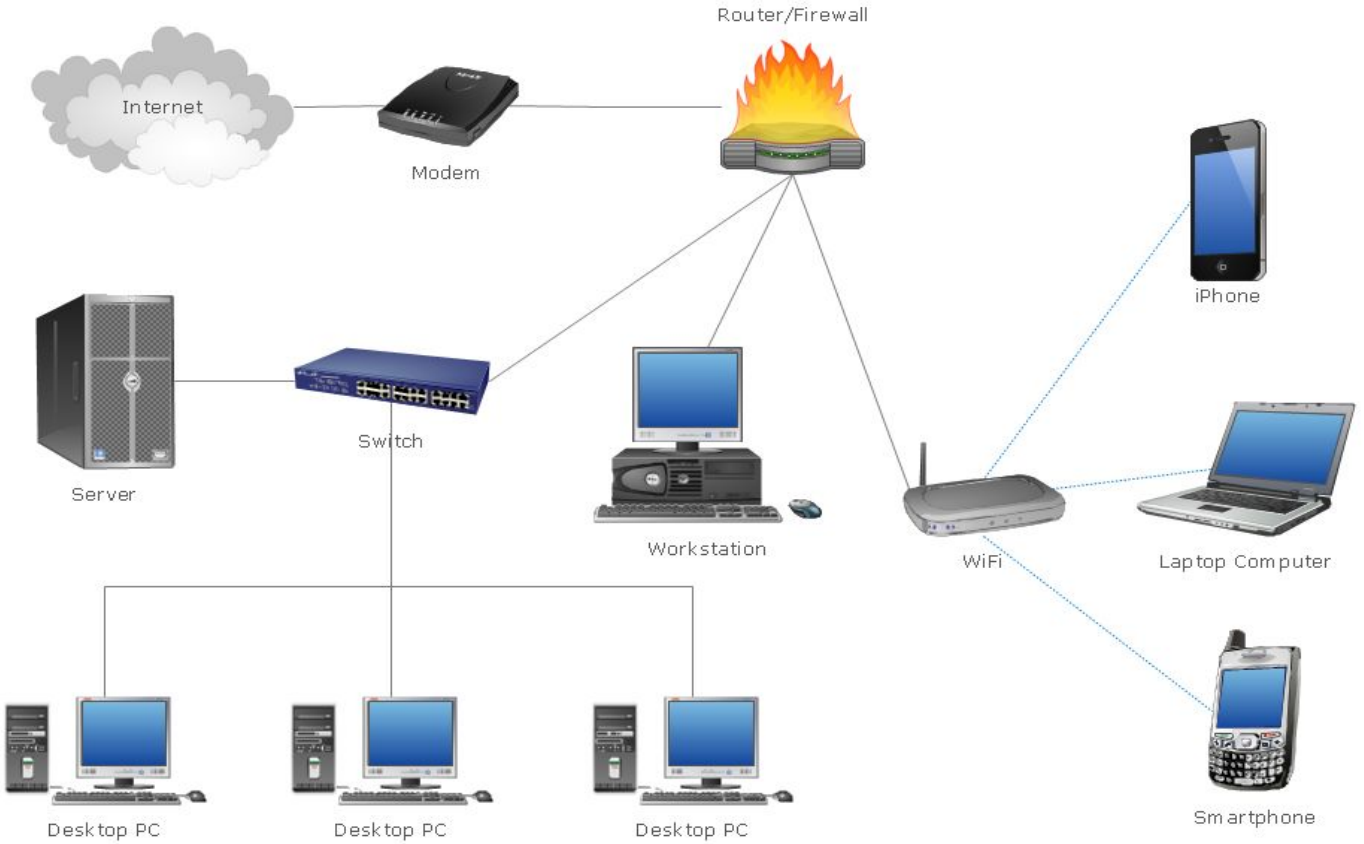
- **LAN (Local Area Network):** rete che collega più computer estesa su un'area limitata (es. azienda, ufficio, scuola, abitazione). I cavi di una rete LAN non attraversano il suolo pubblico.
- **WLAN (Wireless Local Area Network):** tipologia di rete LAN dove i dispositivi sono collegati in modalità wireless

Architettura centralizzata o distribuita

- **CENTRALIZZATA**: prima architettura utilizzata, unico grande computer centrale con tanti terminali “stupidi” collegati

- **DISTRIBUITA**: si diffonde grazie al minor costo dei componenti hardware; più computer, dotati di capacità di elaborazione e di memoria, connessi tra di loro per **condividere** informazioni, software e componenti hardware e per **comunicare**. Le risorse (hardware e software) sono distribuite tra le diverse macchine

Esempio di una rete WLAN



Dispositivi di rete

- **Hub, Switch, Router:** dispositivi che, a vari livelli, permettono il collegamento di più macchine all'interno di una rete
- **Firewall:** (in italiano, muro tagliafuoco) è un componente, hardware o software, di una rete informatica che controlla gli accessi filtrando il traffico in entrata e in uscita
- **Access point:** dispositivo che consente a un utente di accedere in modalità wireless a una rete cablata

Configurare un access point

Prerequisiti

- Connessione a internet
- Router wireless o Access point collegato alla rete cablata
- Dispositivi wireless dotati di:
  - schede interne PCI
  - schede esterne USB

Collegarsi all'access point

PRIMO COLLEGAMENTO PER LA CONFIGURAZIONE

- Utilizzare preferibilmente un cavo di rete piuttosto che un collegamento wireles
- Digitare nel browser l'indirizzo dell'access point, di solito:
  - 192.168.0.1
  - 10.1.1.1
- Cos'è un indirizzo IP?

Abilitare DHCP

Dynamic Host Configuration Protocol (protocollo di configurazione IP dinamico)

Indicare il range degli indirizzi IP da assegnare e quindi il numero massimo degli utenti

CONFIGURAZIONE LAN

Questa sezione consente di configurare le impostazioni della rete locale connessa al router. Questa sezione è facoltativa. Per un corretto funzionamento della rete non dovrebbe essere necessaria alcuna modifica delle impostazioni.

IMPOSTAZIONI ROUTER

In questa sezione è possibile configurare le impostazioni della rete locale per il router. L'indirizzo IP configurato in questo contesto corrisponde all'indirizzo IP utilizzato per accedere all'interfaccia di gestione basata sul Web. Se si modifica l'indirizzo IP, è necessario aggiornare le impostazioni di rete del PC per poter accedere nuovamente alla rete.

Indirizzo IP router :	192.168.1.1
Subnet mask :	255.255.255.0

IMPOSTAZIONI DEL SERVER DHCP (FACOLTATIVO)

In questa sezione è possibile configurare il server DHCP integrato in modo da assegnare automaticamente gli indirizzi IP ai computer della rete.

Abilita server DHCP :	☑	
Intervallo di indirizzi IP DHCP :	192.168.1.2	- 192.168.1.254
Tempo di validità DHCP :	24	(ore)
Relay DHCP :	☐	
Indirizzo IP server DHCP :		

Sicurezza access point

Evitare che le persone non autorizzate possano connettersi

Strumenti:

- Nascondere la rete
- Crittografia
- Permettere l’accesso solo a IP autorizzati
- Controllo parentale (se disponibile)

Nascondere la rete

Nascondere la rete impostando il flag Hidden SSID o Nascondi SSID o Invisibile. In tal modo la rete non sarà inclusa nell'elenco delle reti visualizzato quando i client wireless effettuano la scansione delle reti disponibili. Per collegare i dispositivi wireless al router sarà necessario immettere manualmente il nome della rete wireless (SSID) in ogni dispositivo.

Crittografia (algoritmi di cifratura)

- **WEP** (Wired Equivalent Privacy): primo standard per reti Wi-Fi, per questo algoritmo sono emerse alcune debolezze
- **WAP**: supera i difetti del precedente ed è compatibile con le stesse reti (da utilizzare per dispositivi meno recenti)
- **WAP2**: evoluzione del precedente, maggiore sicurezza, per dispositivi recenti

Il WAP e il WAP2 possono essere utilizzati insieme per bilanciare protezione e compatibilità in modo ottimale

La password

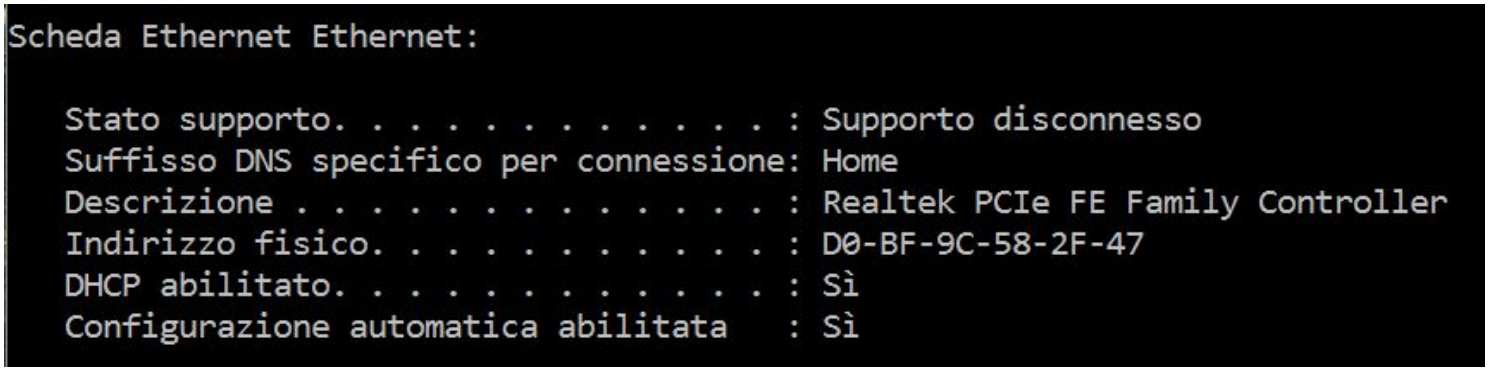
- Composta da lettere, numeri e caratteri speciali (es: * / ! ?)
- Sufficientemente lunga (lunghezza massima chiave WAP2 64 caratteri)

Suggerimento:

- Utilizza le iniziali di una frase o di un proverbio e intervallale a dei numeri
- Esempio: Nel Mezzo Del Cammin Di Nostra Vita
- Password: n1m2d3c4d5n6v7

Permettere l'accesso solo a IP autorizzati

- Ogni dispositivo possiede un proprio MAC address (sequenza di 6 coppie di numeri che identifica univocamente una scheda di rete)
- Per individuare il MAC address di un pc digitare: **ipconfig /all** dal prompt del dos



- Abilitare nel router o nell'access point il dispositivo

Controllo parentale

- Disponibile su alcuni dispositivi
- Funzione: **blocco siti web**. Consente di creare rapidamente un elenco di siti Web ai quali gli utenti non possono accedere
- Funzione: **limitazione ora accesso internet**. Consente di controllare quando i client o i PC connessi al router sono autorizzati ad accedere a Internet
- Le due funzioni possono essere utilizzate contemporaneamente; ad esempio è possibile bloccare un sito web un giorno della settimana in un determinato orario

Infine

Se non utilizzate l’access point: **spegnetelo!**

Si evitano gli attacchi alla rete che comportano il susseguirsi di operazioni che possono protrarsi per giorni o settimane

Sicurezza di un sistema distribuito

Problemi alla sicurezza di un sistema

- **Fattori non umani:** Interruzione energia, guasti hardware o software, incendi, calamità naturali, guerre ecc.
- **Fattori umani:**
  - **Interni**. Azioni volontarie o involontarie causate da dipendenti e/o persone autorizzate
  - **Esterni**. Cracker. Attacchi con virus, trojan, malware (software dannoso) ecc.

Cracker (o Black Hat Hacker)

“Persona che si ingegna per eludere blocchi imposti da qualsiasi sistema informatico al fine di trarne profitto o creare danni” (wikipedia)

Si contrappone a **Hacker (o White Hat Hacker)**: “è un esperto di sistemi informatici e di sicurezza informatica in grado di introdursi in reti informatiche protette e in generale di acquisire un'approfondita conoscenza del sistema sul quale interviene, per poi essere in grado di accedervi o adattarlo alle proprie esigenze” (wikipedia)

Vulnerabilità e tipi di attacchi

- Fragilità della password (può essere sottoposta ad attacchi **bruteforce**)
- Ottenere i **privilegi dell'amministratore** attraverso la scoperta della password di sistema
- Installare applicativi come **trojan** o **back door** che permettono, in un secondo tempo, di prendere il controllo del controllo del sistema

L'aggressore spesso occulta le tracce cancellando i dati nei **log di sistema**

Tipologie di attacchi

- **Denial of Service (DoS)**: portare un sistema al limite delle proprie capacità attraverso la manipolazione dei parametri in ingresso (es. inondare un server di posta elettronica)
- **Distributed Denial of Service (DDoS)**: funzionamento analogo al precedente, ma utilizzando numerose macchine attaccanti
- **Distributed Reflection Denial of Service (DRDoS)**: simile ai precedenti con la particolarità di far credere al server ricevente che il mittente dell'attacco è il server stesso. Si ottiene un effetto moltiplicatore delle richieste al server.

Tipologie di attacchi

- **Sniffing**: intercettare i pacchetti che circolano in rete allo scopo di leggere le informazioni
- **IP Spoofing**: si invia un pacchetto a una macchina falsificando l'IP del mittente. Tecnica utilizzata per superare alcune difese sulle intrusioni
- **Phishing**: truffa con la quale si cerca di ingannare una persona convincendola a fornire informazioni personali fingendosi un ente affidabile

Metodi di difesa attivi

- Aggiornare i componenti hardware e software (chi intende entrare in un sistema informativo cerca di sfruttare vulnerabilità vecchie piuttosto che trovarne delle nuove);
- Utilizzare la crittografia, una corretta gestione delle password e delle autorizzazioni soprattutto per reti WiFi (vedi diapositiva su “Sicurezza Access Point”)
- Utilizzare un **firewall** che garantisca il controllo degli accessi controllando tutto il traffico che lo attraversa

FIREWALL (muro contro il fuoco)

DEFINIZIONE: insieme delle difese perimetrali, hardware e software, di un sistema informatico

- controlla gli accessi alla rete controllando i pacchetti in ingresso e in uscita in base agli IP di provenienza o destinazione (filtraggio)
- regola: permettere ciò che deve passare e fermare tutto il resto
- questo filtraggio è presente in quasi tutti i router o i sistemi operativi
    - punto già trattato in precedenza

Disaster Recovery Plan

Piano che permetta di ripristinare il normale funzionamento del sistema

Soluzioni possibili:

- **Backup e restore**: copia e ripristino di archivi di grandi dimensioni
- **Mirroring**: unità di memoria con copie identiche dello stesso disco
- **Duplexing**: duplicazione unità controllo dei dischi oltre che dei dischi
- **Duplicazione intero sistema**: duplicazione del server
- **RAID** (Redundant Array of Inexpensive Disk): distribuire i dati su più dischi per permette la ricostruzione tramite algoritmi di quelli eventualmente persi

Codice della Privacy

(Decreto Legislativo 30 giugno 2003 n. 196)

Parametri di sicurezza

- **INTEGRITA'**: i dati non devono essere alterati (cancellati o modificati) da terzi non autorizzati o a causa di eventi accidentali o naturali
- **RISERVATEZZA**: ridurre il rischio di accesso improprio e all'utilizzazione da parte di soggetti non autorizzati; occorre prevedere meccanismi di autenticazione
- **DISPONIBILITA'**: ridurre il rischio di impedimento agli utenti autorizzati di fruire del sistema o di accedere alle informazioni

Definizioni (dal Codice della Privacy)

- **TITOLARE**: la persona fisica, la persona giuridica ... cui competono ... le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza; nelle scuole il Dirigente Scolastico quale legale rappresentante;
- **RESPONSABILE**: la persona fisica, la persona giuridica ... preposti dal titolare al trattamento di dati personali; figura delegata dal DS in genere il DSGA o un impiegato amministrativo;
- **INCARICATO**: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- **INTERESSATO**: persona fisica cui si riferiscono i dati personali.

Misure minime (allegato B codice privacy)

- L’intervento tecnico e organizzativo volto a prevenire, contrastare o ridurre i rischi individuati, oltre alle attività volte a verificare e a controllare nel tempo il corretto uso del trattamento dei dati;
  - **autenticazione** informatica;
  - adozione di procedure di **gestione delle credenziali** di autenticazione;
  - utilizzazione di un **sistema di autorizzazione**;
  - **aggiornamento periodico** dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
  - **protezione degli strumenti elettronici** e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
  - adozione di procedure per la **custodia di copie di sicurezza**, il ripristino della disponibilità dei dati e dei sistemi;
  - **adozione di tecniche di cifratura** o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Misure minime (allegato B codice privacy)

IN SINTESI:

- Prevedere un sistema di autenticazione che permetta di risalire in caso di controversie legali e di utilizzo non conforme al responsabile delle azioni dannose;
- Il sistema dovrà essere mantenuto aggiornato sia per quanto riguarda l'hardware che il software;
- Predisporre un sistema di ripristino dei dati persi (Disaster Recovery Plan)
- Redigere e aggiornare il D.P.S. (Documento Programmatico sulla Sicurezza).

Autenticazione

- Accesso tramite username e password o budge, pass ecc.
- Robustezza della password
- Scadenza password ogni 6 mesi (3 mesi per i dati sensibili)
- Istruzioni agli incaricati per non lasciare incustoditi gli strumenti elettronici quando si allontanano dalle loro postazioni e per assicurare la diligente segretezza delle credenziali di accesso o la custodia dei dispositivi

Policy di sicurezza

Policy di sicurezza

Documento nel quale sono contenute tutte le disposizioni, i comportamenti e le misure organizzative richieste ai dipendenti e ai collaboratori aziendali (nelle scuole: personale ata, docenti e alunni) per contrastare i rischi informatici

Caratteristiche

- **AGGIORNATE**: sia per riflettere i cambiamenti della rete che del suo uso (sempre più dispositivi mobili)
- **COMPRENDERE TUTTI GLI ASPETTI**: dall'accesso ai locali all'uso della rete
- **BILANCIARE SICUREZZA E PRODUTTIVITA'**: le policy troppo severe ostacolano il lavoro
- **CHIARE**: scritte in modo chiaro, tali da essere facilmente comprese, utilizzare pochi termini tecnici
- **CONOSCIUTE**: se nessuno le conoscere sono inutili; informare dei rischi piuttosto che esporre semplicemente le regole
- **ATTUATE**: prevedere controlli a vari livelli e sanzioni per le infrazioni

Alcuni punti da sviluppare

- Utilizzo del Personal Computer e dei dispositivi mobili
- Utilizzo della rete
- Gestione delle Password
- Uso della posta elettronica
- Uso della rete Internet e dei relativi servizi
- Protezione antivirus
- Osservanza delle disposizioni in materia di Privacy
- Sanzioni
- Aggiornamento e revisione

Alcuni esempi trovati in rete

AZIENDE

- Esempio di regolamento aziendale (napolifirewall.com)
- Policy strumentazioni informatiche (daycoeurope.com)
- Regolamento informatico (assoprivacy.net)

SCUOLE

- icviatrionfale.gov.it
- icsocrate.it
- iiscremona.gov.it
- comprensivocassino1.gov.it

Attività pratica

Policy di sicurezza

Predisposizione di un protocollo per la sicurezza

lavoro di gruppo in condivisione

Cyberbullismo

Definizione

Uso delle nuove tecnologie per intimorire, molestare, mettere in imbarazzo, far sentire a disagio o escludere altre persone (http://www.azzurro.it/en/node/112)

cyberbullismo-fabrizio-pillotto

Differenze rispetto al bullismo tradizionale

- **Anonimo**: anche se illusorio
- **Difficile reperibilità**: uso della messaggistica istantanea e dei forum rende difficile reperirlo e rimediarvi
- **Indebolimento delle remore etiche**: spesso la gente fa e dice online cose che non farebbe o direbbe nella vita reale; manca la consapevolezza degli effetti delle proprie azioni
- **Assenza dei limiti spazio-temporali**: investe la vittima ogni volta che si collega al mezzo elettronico (https://it.wikipedia.org/wiki/Cyberbullismo)

“A differenza di quanto accadeva nel tradizionale bullismo in cui le vittime, rientrate a casa, trovavano, quasi sempre, un rifugio sicuro, un luogo che le proteggeva dall’ostilità e dalle angherie dei compagni di scuola, nel cyberbullismo le persecuzioni possono non terminare mai”. (http://www.cyberbullismo.com/definizioni-e-proprieta)

Ruolo degli spettatori

I “compagni” che assistono alle vessazioni online possono assumere una funzione:

- PASSIVA: si limitano a rilevare nelle proprie email, chat atti di bullismo diretti a altri
- ATTIVA: scaricano, commentano, votano, condividono diventando di fatto dei bulli loro stessi. Il comportamento attivo può essere anche sollecitato dal cyberbullo

Tipologie di cyberbullismo

- **FLAMING**: (da flame = fiamma) messaggi elettronici violenti e volgari di durata temporale limitata, volti a suscitare conflitti verbali all'interno di una rete; ad esempio diretti contro i principianti a un videogioco
- **HARASSMENT**: (harassment = molestia) messaggi scortesi, offensivi, insultanti ripetuti nel tempo. Caratteristiche: persistenza e asimmetria tra bullo e vittima.
- **CYBERSTALKING**: si verifica quando harassment diventa particolarmente insistente e intimidatorio. Il comportamento aggressivo diventa una persecuzione. La vittima teme anche per la propria incolumità fisica. Il bullo può arrivare a diffondere anche materiale riservato sulla vittima.
- **DENIGRATION**: diffusione di messaggi falsi o dispregiativi (pettegolezzi, immagini modificate) allo scopo di danneggiare la reputazione della vittima. Può anche essere utilizzata dagli studenti per danneggiare i propri docenti.

Tipologie di cyberbullismo

- **IMPERSONATION**: il bullo viola l'identità della vittima (es. ha ottenuto la password) o simula un'altra identità per inviare a suo nome messaggi offensivi
- **OUTING e TRICKERY**: (trickery = inganno, outing = uscita) il bullo entra prima in confidenza con la vittima, scambiando con essa informazioni intime e/o private, e poi le diffonde tramite mezzi elettronici come internet, sms, etc.
- **EXCLUSION**: escludere intenzionalmente un'altra persona da un gruppo di amici, da una chat o da un gioco
- **CYBER-BASHING** O **HAPPY SLAPPING**: (da slap = schiaffo) uno o più ragazzi si riprendono mentre picchiano o schiaffeggiano un coetaneo e poi pubblica le immagini in internet.

Aspetti legali

(Circolare 30 Novembre 2007, Ministero della Pubblica Istruzione)

La circolare prescrive chi effettua fotografie o registrazioni e intende divulgarle deve:

- informare la persona interessata (privacy)
- acquisire il consenso espresso (se dati sensibili consenso in forma scritta)

Per l'inosservanza sono previste sanzioni amministrative che vanno da 3.000 a 18.000 euro (per i dati sensibili da 5.000 a 30.000 euro)

Aspetti legali

(Circolare 30 Novembre 2007, Ministero della Pubblica Istruzione)

I seguenti casi vanno segnalati all'Autorità Giudiziaria (**illeciti penali**):

- Indebita raccolta, rivelazione e diffusione di immagini attinenti alla vita privata che si svolgono in abitazioni altrui o in altri luoghi di privata dimora (art. 615 bis c.p.)
- il possibile reato di ingiurie, in caso di particolari messaggi inviati per offendere l'onore o il decoro del destinatario (art. 594 c.p.)
- le pubblicazioni oscene (art. 528 c.p.)
- la tutela dei minori riguardo al materiale pornografico (art. 600-ter c.p.; l. 3/8/98, n. 269)

Aspetti legali

Autore del reato minorenne: la competenza è del Tribunale per i minorenni e procede la Procura della Repubblica presso tale Tribunale

Autore del reato maggiorenne: la competenza è del Tribunale ordinario e procede la Procura della Repubblica presso tale Tribunale

Ruolo degli insegnanti

- PREVENZIONE: fornire educazione e informazione per sensibilizzare i ragazzi:
  - i ragazzi potrebbero ritenere scherzi dei veri e propri reati
  - spesso le vittime del cyberbullismo spesso non si rendono conto delle conseguenze e tendono a minimizzare, “normalizzare” i comportamenti
  - l’apparente distacco, creato dal mezzo informatico, lascia meno tempo alla riflessione; il bullo non vede le conseguenze del proprio comportamento
  - gli studenti potrebbero non denunciare il cyberbullismo anche in conseguenza delle sanzioni (tolto lo smartphone o vedersi ridicolizzati)
- Aiutare i ragazzi che si trovano in difficoltà
- Intervenire con chi utilizza le rete impropriamente

Le 10 regole della polizia postale

1. **Proteggere il dispositivo che si utilizza per accedere a Internet**: aggiornare il software, usare antivirus e firewall
2. **Proteggere la password**: lunghezza, utilizzare caratteri speciali e numeri, cambiarla periodicamente
3. **Utilizzare reti sicure**: attenzione a usare le wifi gratuite in locali pubblici
4. **Proteggere le informazioni personali**: controllare se la pagina è sicura (cifratura, https) quando si inseriscono informazioni personali
5. **Evitare le truffe**: attenzione a cliccare su link con premi o ad aprire messaggi dalla posta elettronica

Le 10 regole della polizia postale

6. **Prevenire il furto di identità**: diffidare dei messaggi o dei siti che chiedono dati finanziari o personali
7. **Usare i social network con prudenza e rispetto**: nei profili dei social network limitare i dati personali e utilizzare le impostazioni per la privacy
8. **Non rispondere alle provocazioni**: non rispondere alle email o alle chat con messaggi provocatori
9. **Segnalare i contenuti illeciti o inappropriati**: segnalare i contenuti illeciti per consentire un'esperienza di navigazione migliore per tutti
10. **Bloccare i siti ritenuti inadatti ai bambini e adolescenti**: regola per i genitori e gli adulti; bloccare alcuni contenuti per insegnare ai ragazzi un consumo critico della rete

Attività pratica

Regole per contrastare il cyberbullismo

Predisposizione di un insieme di regole per contrastare il fenomeno del cyberbullismo

lavoro di gruppo in condivisione