Sicurezza in rete: comportamenti furbi

Password sicura!

la password dovrebbe essere lunga almeno 8 caratteri e composta sia di lettere che di numeri e non riconducibile a informazioni facilmente collegabili alla nostra persona (es. data di nascita o matrimonio, …); non riveliamo a nessuno la nostra password (unica eccezione la password dei bambini più piccoli che deve essere condivisa con i genitori) e non scriviamola nella rubrica del cellulare o nel quaderno degli appunti che teniamo di fianco al pc; utilizziamo password diverse tra un sito e l'altro e tra il router e la rete wireless domestica; ricordiamoci che sul web si trovano facilmente e gratuitamente programmi che ci possono aiutare generando password complesse e archiviandole in modalità sicura sul nostro pc o il nostro smartphone

..ma non solo: domanda di riserva sicura!

chi cerca di entrare nel nostro account può utilizzare il link "Hai dimenticato la password?"; spesso le risposte a queste domande sono rintracciabili nei contenuti che abbiamo postato sul web – es. nome del cane, scuola frequentata, marca di birra preferita…

Postiamo con la testa!

consideriamo sempre che tutto quello che inseriamo nei social network può essere "per sempre": anche se eliminassimo il nostro account i nostri amici hanno avuto la possibilità nel tempo di scaricare, salvare o condividere i nostri commenti o le nostre foto; ricordiamoci poi che la cancellazione definitiva del dato è un'operazione difficile e costosa, tanto che per i provider di servizi garantirne la reale esecuzione è al limite dell'impossibile

Amicizie selettive!

nell'accettare o nel cercare amicizia sui social network, ricordiamoci del "numero di Dunbar": è impossibile avere centinaia e centinaia di veri amici; pensiamo sempre se al potenziale amico vorremmo dare davvero tutte le informazioni che postiamo sul web

Dubitiamo del mittente!

evitiamo di dare per scontato che i messaggi siano veramente inviati dal nome che ci appare; quando sospettiamo che un messaggio sia fraudolento, cerchiamo un metodo alternativo per contattare il mittente e verificare la provenienza del messaggio o dell'invito ad un nuovo social network

Clikkiamo con attenzione!

trattiamo i link che riceviamo dai nostri amici sui social network allo stesso modo di quelli contenuti nelle e-mail; facciamo attenzione ai messaggi di vincite straordinarie o incredibile fortuna: spesso celano sorprese spiacevoli

Digitare è meglio che clikkare!

raggiungiamo le nostre pagine personali digitando direttamente l'indirizzo del social network nel browser o usando i segnalibri personali: fare click su un link ci espone al rischio di immettere nome e password dell'account in un sito falso, è quello che si chiama "phishing"

Sicurezza in rete: tecnologia amica

Attenzione alle trappole!

a volte possiamo essere vittime di attacchi che sfruttano le nostre paure e la nostra buona fede: evitiamo di scaricare (download) programmi che non riconosciamo a seguito di pop up o messaggi anche se affermano di proteggere il nostro PC o di rimuovere virus individuati sulla nostra macchina, è molto probabile che facciano l'esatto contrario; in generale cerchiamo di scaricare software esclusivamente da siti affidabili e diffidiamo delle offerte gratuite di musica, giochi, video e premi; usiamo cautela nell'aprire allegati o fare clic su link contenuti nelle email, riportati in chat, postati sui social network o riportati nei banner pubblicitari (evitiamo quindi di clikkare su "Avanti", "OK" o "Accetto"): se abbiamo dei dubbi chiudiamo il browser chiudendo, alla relativa richiesta, tutte le schede senza salvarle per il successivo riavvio del browser.

Pesiamo le App!

valutiamo bene le "App" che scarichiamo sulla nostra pagina social o sui nostri smartphone: spesso le app possono accedono senza che ce ne accorgiamo alle informazioni del nostro pc, tablet o smartphone; quando diamo l'ok al download leggiamo in fondo al disclaimer le tipologie di dati cui le app richiedono l'accesso e valutiamo se ciò sia realmente necessario

Scegliamo noi la nuvola!

analizziamo bene i siti su cui salviamo periodicamente i nostri dati: il salvataggio remoto mediante tecnologia "cloud" può essere più comodo e semplice della copia su disco fisso esterno; non tutti i siti però forniscono i medesimi livelli di sicurezza, quali ad esempio la protezione (cifratura) del canale con cui si caricano e scaricano i dati

Chiudiamo a chiave il wi-fi!

le connessioni non protette sono una facile sorgente di informazioni gratuite: proteggiamo la nostra rete con le chiavi di sicurezza e diffidiamo delle reti libere che troviamo per strada

Antivirus forever!

usiamo e aggiorniamo l'antivirus sia sui pc che sugli smartphone: virus, worm e trojan sono programmi insidiosi che possono manipolare il nostro computer e i spiare o anche cancellare i dati memorizzati; impostiamo aggiornamenti automatici e scansioni continue e periodiche - sebbene a volte possa sembrare che questo causi rallentamenti o perdite di tempo: l'antivirus è il primo livello di protezione dei nostri strumenti, come le guardie sugli spalti del nostro castello

Proteggiamoci con il Firewall!

il firewall è un programma, spesso integrato nel sistema operativo o negli antivirus, che lascia passare sia in entrata che in uscita solamente i dati che hanno il nostro permesso: attiviamolo; il firewall è come le mura del nostro castello

Software sempre aggiornato!

quando i produttori scoprono un punto debole nel loro software pubblicano un update (o patch) per impedire che gli hacker possano sfruttare questa falla: acconsentiamo alle richieste di update, sembra una noia ma non lo è

Sicurezza in rete: navigazione "social-MENTE" attiva

Impariamo a conoscere i Social network!

scegliamo i social network con attenzione e leggiamone l'informativa sulla privacy: possiamo scoprire cose interessanti e curiose sulle modalità con cui questi siti trattano i nostri dati

Un solo amministratore per tutti, un'utenza per ognuno!

Sul pc, preferiamo lavorare con utenze che non abbiano diritti di amministratore, chi ci "ruba" l'utenza eredita i diritti ad essa connessi – ad esempio, se prendiamo un virus quando siamo connessi come amministratori, questo virus avrà i diritti di amministratore sulla nostra macchina; se il pc o il tablet sono condivisi, creiamo un utenza per ognuna delle persone che ci accedono: anche questo diminuisce il rischio di perdita dei dati e permette livelli di protezione più precisi

Impostiamo correttamente i livelli di privacy dei browser!

tutti i browser danno la possibilità di alzare o abbassare i livelli di protezione della privacy: a livelli più alti corrispondono funzionalità più limitate e viceversa, è quindi importante trovare il giusto equilibrio per ogni utente (ad esempio più alto per i ragazzi, minore per gli adulti); le modalità di impostazione variano da prodotto a prodotto ma possono essere facilmente trovate curiosando un po' nei menù a tendina

Navighiamo in sicurezza!

impostiamo la sicurezza di google e di youtube al massimo livello per ridurre la possibilità che, per errore, durante la navigazione ci si imbatta in immagini e video non adatti o sgradevoli; blocchiamo poi la visualizzazione delle finestre popup utilizzando le funzionalità di blocco integrati nei browser;

Mettiamoci in gioco!

parliamo con i nostri ragazzi della loro e della nostra vita sul web, mostriamo interesse verso le loro attività online e discutiamo dei problemi ma anche delle numerosissime e divertenti cose che è possibile fare con il Web; impariamo anche noi ad utilizzare maggiormente Internet e chiediamo ai nostri ragazzi consigli sull'utilizzo dei diversi strumenti strumenti: ammettere i nostri limiti tecnologici può aiutare a creare un momento di condivisione senza perdere il ruolo di educatore; discutiamo con loro di ciò che è più opportuno fare in caso di situazioni sgradevoli anche se queste non si sono mai avverate

Navighiamo insieme ai ragazzi!

creiamoci delle occasioni per navigare insieme ai ragazzi: ad esempio pianifichiamo insieme un viaggio, cerchiamo siti relativi ai loro hobby: navigando insieme possiamo aiutare i nostri ragazzi a valutare il valore delle informazioni trovate

Sicurezza in rete: aiutiamo i nostri ragazzi 1/2

1. più sono piccoli più cerchiamo di **essere presenti** quando i ragazzi usano Internet;
2. stabiliamo delle **regole precise** per l'utilizzo di Internet (tempi, modi, …);
3. raccomandiamogli di **non condividere informazioni personali** come nome, indirizzo, numero di telefono o password con gli altri utenti di Internet; le foto e altre informazioni private non dovrebbero mai essere condivise con utenti che si conoscono solo online;
4. facciamogli capire che è corretto **condividere sul web foto, immagini e informazioni dei propri amici solo con il loro consenso**
5. quando ci chiedono di attivare il loro primo account sui social network **facciamoci dare la loro amicizia**: più che un controllo è un modo semplice di aiutarli e dar dei consigli sul loro comportamento; ricordiamoci che per registrarsi in facebook è necessario aver compiuto almeno i 13 anni;
6. quando costretto a registrarsi sui siti, magari per giocare, aiutiamolo a crearsi **un'utenza che non riveli alcuna informazione personale** – soprattutto età o sesso; nel form di registrazione indichiamo l'indirizzo mail di un adulto;
7. usiamo gli strumenti di "**parental control**" per creare profili appropriati e filtrare i contenuti di Internet, ma ricordiamoci che **questi strumenti sono solo un aiuto ma non sono sufficienti a proteggerlo;**
8. incoraggiamoli **a spiegarci se qualcosa o qualcuno in Internet li fa sentire a disagio** o minacciati: facciamogli capire che se hanno dei dubbi siamo a loro disposizione per parlarne subito;
9. ricordiamogli che è meglio che **interrompano subito** qualunque comunicazione (via e-mail, chat, instant messaging) se qualcuno inizia a rivolgere loro domande troppo personali o dal contenuto sessuale;
10. suggeriamogli di **"chattare" nell'area pubblica** evitando le chat private dove non è possibile monitorare le conversazioni (aree "whisper"); suggeriamogli anche di evitare di rivelare nelle chat o nei forum informazioni personali (tra cui età e sesso) o informazioni sulla famiglia;
11. usiamo noi internet in sicurezza consapevoli di essere un **modello di riferimento** per i più piccoli;
12. diamo **priorità alle loro richieste** e al loro desiderio di parlarci della loro vita in rete: le altre nostre attività possono aspettare;
13. informiamoci sui **siti Web visitati dai nostri ragazzi** e sugli utenti con cui parlano;
14. insistiamo sul concetto che non debbano **mai incontrare di persona da soli un amico conosciuto online**, e poi insistiamo ancora; nel caso, accompagniamoli noi o – nel peggiore dei casi - assicuriamoci che vadano all'incontro accompagnati da amici; l'incontro deve sempre avvenire in un luogo pubblico;
15. insegniamo ai ragazzi a **scaricare** programmi, musica o file **solo con l'autorizzazione di un adulto** (la condivisione e l'utilizzo di file può essere illegale);
16. parliamo con i nostri ragazzi adolescenti dei contenuti online per adulti e della pornografia: indirizziamoli verso **siti adatti, dedicati alla salute e alla sessualità;**

Sicurezza in rete: aiutiamo i nostri ragazzi 2/2

17. aiutiamoli a proteggersi dallo spam: raccomandiamogli di non condividere il proprio indirizzo e-mail online e di **non rispondere alla posta indesiderata;**
18. valorizziamo, anche con il nostro comportamento e linguaggio, un **comportamento online etico e responsabile**; facciamo in modo che non utilizzino Internet per diffondere pettegolezzi, rendersi protagonisti di cyber-bullismo, insultare, offendere o minacciare altri utenti;
19. parliamo con loro anche del **gioco d'azzardo online** e dei potenziali rischi di questa attività: tra l'altro il gioco d'azzardo dei minorenni – anche online - è illegale
20. condividiamo con loro che **"crakkare", "jailbrekkare" e "roottare" i sistemi dei pc e degli smartphone (in pratica manomettere i sistemi operativi per poter fare più cose) non è una buona idea:** si perde la garanzia sull'acquisto e aumenta la possibilità di essere attaccati dai virus

Mettiamo il computer in uno spazio frequentato da tutta la famiglia!

qualora venissimo a conoscenza che i nostri ragazzi abbiano ricevuto da un contatto online foto o richieste dal contenuto sessuale esplicito, rivolgiamoci immediatamente alla polizia. Conserviamo tutta l'eventuale documentazione, tra cui indirizzi e-mail, indirizzi di siti Web e registri delle chat

Come con la posta normale, usiamo anche una casella postale di famiglia!

creiamo un indirizzo di posta elettronica per tutta la famiglia per registrarsi sul web, creare profili, fare acquisti in Internet e altre attività simili: in questo modo possiamo proteggere il nostro indirizzo di posta elettronica personale prevenendo anche lo spam; aspettiamo a creare indirizzi di posta elettronica personali per i nostri ragazzi quando sono troppo piccoli

Agiamo con fermezza!

qualora venissimo a conoscenza che i nostri ragazzi abbiano ricevuto da un contatto online foto o richieste dal contenuto sessuale esplicito, rivolgiamoci immediatamente alla polizia. Conserviamo tutta l'eventuale documentazione, tra cui indirizzi e-mail, indirizzi di siti Web e registri delle chat

Sentiamoci pronti

parliamo con i nostri ragazzi della loro vita on line con le stesse modalità con cui parliamo normalmente della loro vita reale (amici, attività, delusioni, …);