SECURITY OF THE DIGITAL NATIVES

“ Se pensate che la tecnologia possa risolvere i vostri problemi di sicurreza, allora non capite i problemi e non capite la tecnologia.”

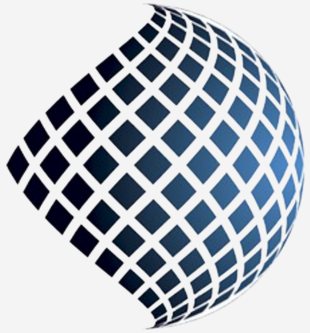
Bruce Schneier

Lo scopo dello studio

Questa indagine ha un duplice obiettivo: da un lato l'attenzione si è concentrata sulla consapevolezza e conoscenza degli studenti universitari per cercare di capire qual è la loro percezione di sicurezza rispetto alla loro conoscenza effettiva, dall'altro si è cercato di delineare il panorama dei possibili rischi sulla base delle loro abitudini, dal modo in cui usano i dispositivi mobili, dal tipo di dati che salvano e dalle funzioni che eseguono.

Chi siamo

Il Tech and Law Center (TLC) è un centro di ricerca multidisciplinare promosso da un gruppo di lavoro composto da membri dell' Università di Milano, Università di Milano–Bicocca, Università dell'Insubria e Politecnico di Milano. Attraverso le attività del centro si vuole promuovere la conoscenza e la comprensione del mondo di Internet e delle nuove tecnologie e della loro interazione con diritto e società.



TECH AND LAW CENTER

The research team

Giuseppe Vaciago
Comitato Esecutivo
Tech and Law

Francesca Bosco
Comitato Esecutivo
Tech and Law

Valeria Ferraris
Ricercatrice
Associazione
Amapola

Pasquale Stirparo
Fellow
Tech and Law

Security of The Digital Natives

TECH AND LAW CENTER

The research team

Stefano Zanero
Comitato Esecutivo
Tech and Law

Pierluigi Perri
Ricercatore
Università di Milano

Davide Ariu
Tech and Law
Fellow

Brikena Memaj
Tech and Law
Membro

Giuseppe Vaciago

Giuseppe Vaciago
Partner presso
R&P Legal

Avvocato a Milano e
Professore di Informatica
Giuridica

Giuseppe Vaciago è un avvocato del foro di Milano dal 2002 e negli ultimi 10 anni il suo obiettivo primario è stato il diritto dell'Information Technology con un focus sulla criminalità informatica. Ha assistito molte aziende nazionali e internazionali operanti nel settore IT. E' autore di numerose pubblicazioni in materia di criminalità informatica, sia su riviste che su testi scientifici, che sono stati adottati dalle Università dove insegna. Accademicamente, ha conseguito il dottorato di ricerca sulla Digital Forensics presso l'Università di Milano ed è docente presso l'Università dell'Insubria (Varese e Como), dove tiene un corso di Informatica Giuridica. Ha anche tenuto numerose conferenze e presentazioni in Italia e all'estero.

Ha frequentato la Fordham Law School e la Stanford Law School come Visiting Scholar per espandere i suoi studi nella propria area di ricerca.

E' membro del comitato esecutivo della Tech e Law Center, ricercatore presso il Centro Nexa e presso il Cybercrime Institute di Colonia.

Twitter: @giuseppevaciago

Francesca Bosco

Francesca Bosco
UNICRI Project
Funzionario del Progetto UNICRI e Dottoranda presso l'Università di Milano Bicocca

Francesca Bosco ha conseguito la laurea in giurisprudenza in diritto internazionale e ha iniziato a lavorare nel 2006 presso UNICRI come membro della Unità Crimini Emergenti. All'interno di questa organizzazione è responsabile dei progetti di prevenzione della criminalità informatica e, in collaborazione con partner strategici, ha sviluppato nuove metodologie e strategie per la ricerca e la lotta contro i crimini informatici.

Recentemente, Francesca si sta occupando dello sviluppo di programmi di rafforzamento delle capacità tecniche per contrastare il coinvolgimento del crimine organizzato in criminalità informatica, nonché sulle implicazioni giuridiche e gli scenari futuri di cyber-terrorismo e guerra cibernetica. Inoltre, esamina e gestisce progetti relativi all'incitamento all'odio on-line e su questioni relative alla protezione dei dati nei casi di profilazione automatica.

Francesca è uno dei fondatori del Tech e Law Center, è nell'Advisory Board del Cybercrime Institute di Colonia ed è attualmente dottoranda presso l'Università di Milano.

Twitter: @francibosco

Pasquale Stirparo

Pasquale Stirparo
Digital Forensics Engineer, fondatore di SefirTech.
Dottorando presso il Royal Institute of Technology (KTH) di Stoccolma.

Pasquale Stirparo è Digital Forensics Engineer e fondatore di SefirTech, una società che si occupa di Mobile Security, Digital Forensics e Incident Response. Prima di fondare SefirTech, Pasquale ha lavorato presso il Joint Research Center (JRC) della Commissione Europea come ricercatore su Digital Forensics e Mobile Security, con particolare interesse per le problematiche di sicurezza e privacy relative ai protocolli di comunicazione dei dispositivi mobili, malware mobile e criminalità informatica. È stato anche impegnato nello sviluppo dello standard “ISO/IEC 27037: Linee guida per l'identificazione, la raccolta e/o l’acquisizione e la conservazione delle prove digitali", per il quale è stato coordinatore nazionale del Working Group ISO27037 nel 2010.

Autore di numerose pubblicazioni scientifiche, è anche stato invitato come relatore a numerosi convegni nazionali ed internazionali e seminari sulla Digital Forensics e docente per il Politecnico di Milano e le Nazioni Unite (UNICRI). Pasquale attualmente è anche studente dottorando presso il Royal Institute of Technology (KTH) di Stoccolma, ha conseguito una Laurea Magistrale in Ingegneria Informatica presso il Politecnico di Torino ed è certificato GCFA, OPST, OWSE, ECCE.

Twitter: @pstirparo

Capitoli del rapporto

ANALISI DEI QUESTIONARI

CONSIDERAZIONI TECNICHE

COSIDERAZIONI GIURIDICHE E DEFINIZIONE DELLE POLICY

CONCLUSIONI E RACCOMANDAZIONI

TECH AND LAW CENTER

Analisi dei questionari

Osservazioni metodologiche

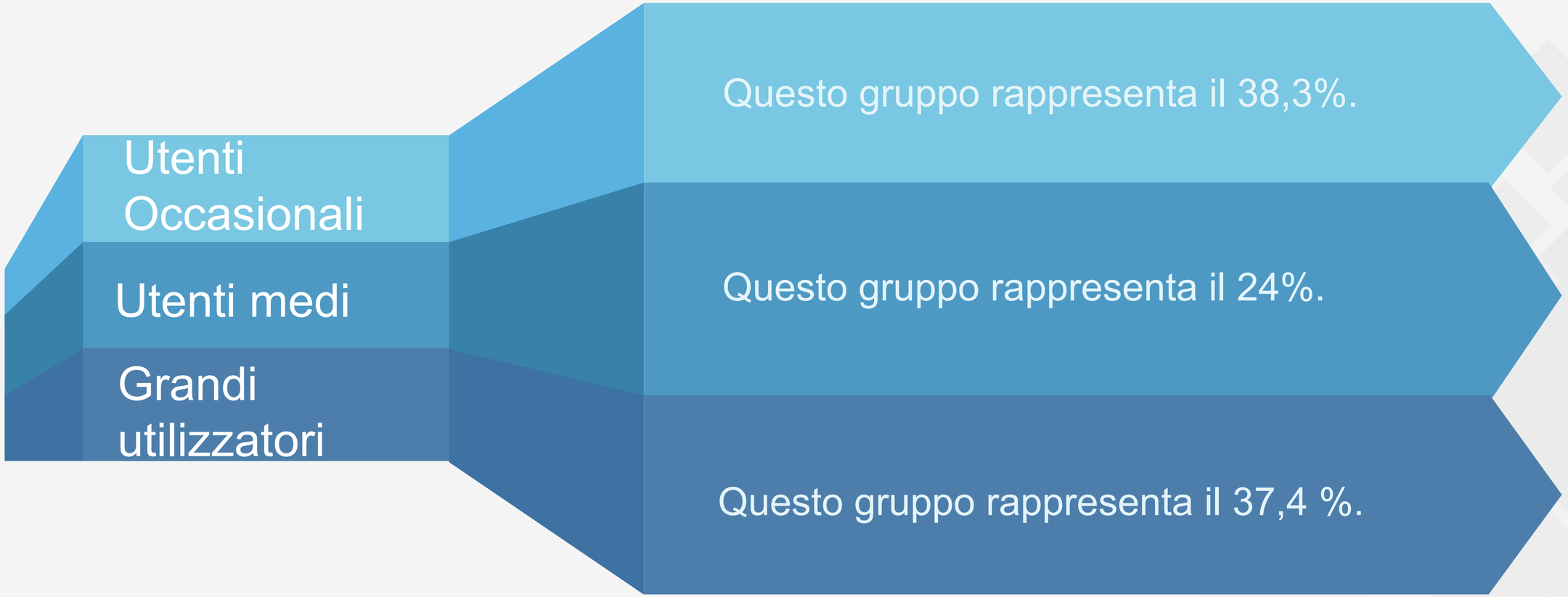
L'indagine è stata condotta utilizzando un questionario contenente 60 domande a risposte multipla suddivise in sezioni relative a vari ambiti: gli utilizzi di smartphone, tablet e computer portatili; gli approcci ai vari tipi di reti, e per tutte le applicazioni dei dispositivi, l'uso di password, la percezione dei rischi per la sicurezza, l'interesse generale e la conoscenza del tema.

I destinatari del questionario sono stati gli studenti universitari di 15 università italiane. La somministrazione del questionario è stata effettuata in modo anonimo attraverso la piattaforma "Google Form", da settembre a novembre 2013.

Sono stati raccolti 1012 questionari. Coloro che hanno risposto provengono da varie aree geografiche e corsi di laurea (con una percentuale omogenea di studenti di materie scientifiche e discipline umanistiche).

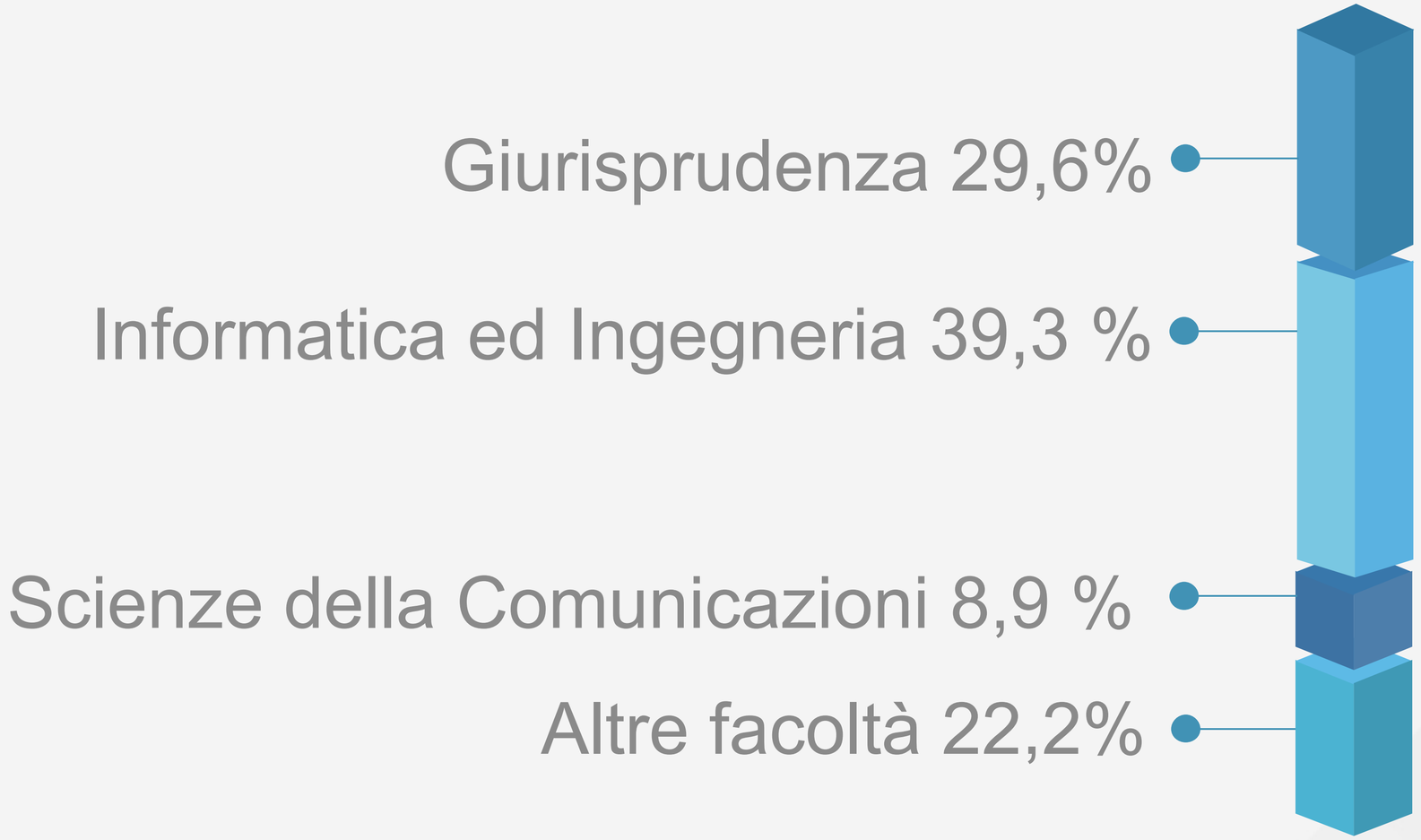
Gruppi di utenti

La tecnica statistica ha aiutato ad identificare tre gruppi ben diversificati. Ognuno di essi presenta caratteristiche omogenee utili per definire i 3 profili utente.



Il campione analizzato: Genere e tipo di studio

Gli utilizzatori di smartphone tablet sono per il 58% maschi e 42% femmine, in linea con la maggiore presenza maschile negli studi informatici.

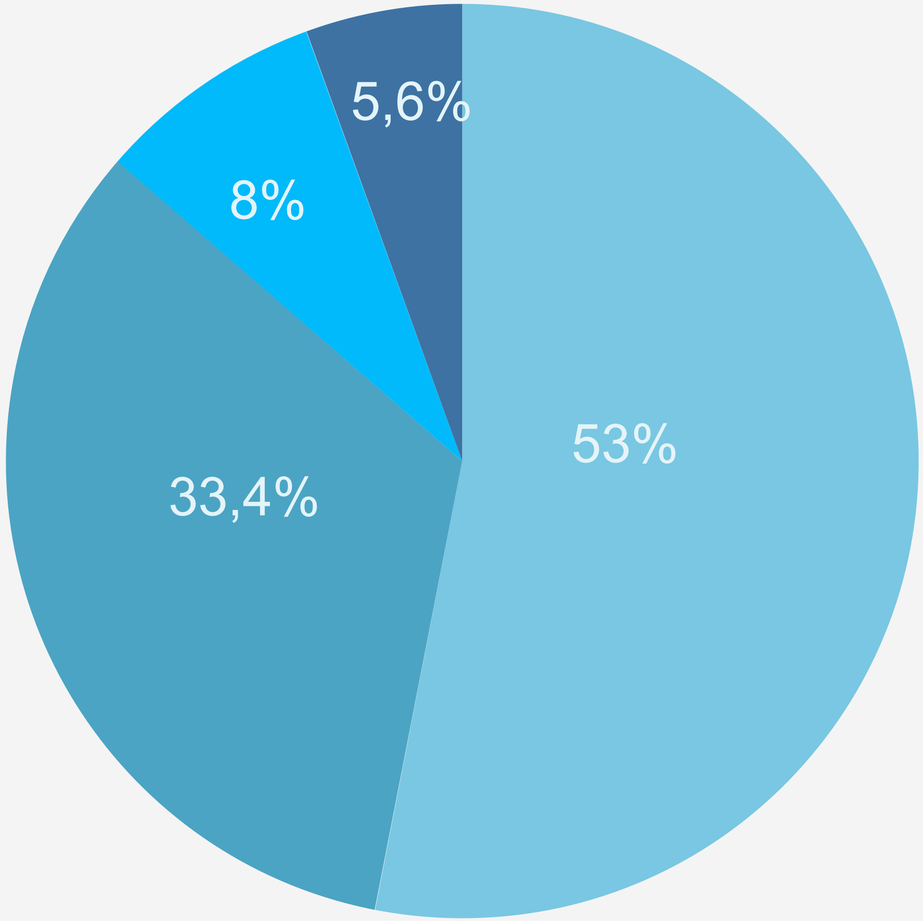


L'utilizzo di dispositivi mobili

Alcune domande preliminari sono finalizzate a comprendere come gli studenti usano i loro dispositivi mobili e quello che salvano sui dispositivi.

La consapevolezza e la paura dei rischi

In che modo sono preoccupati per la sicurezza dei loro dispositivi mobili



Security of The Digital Natives

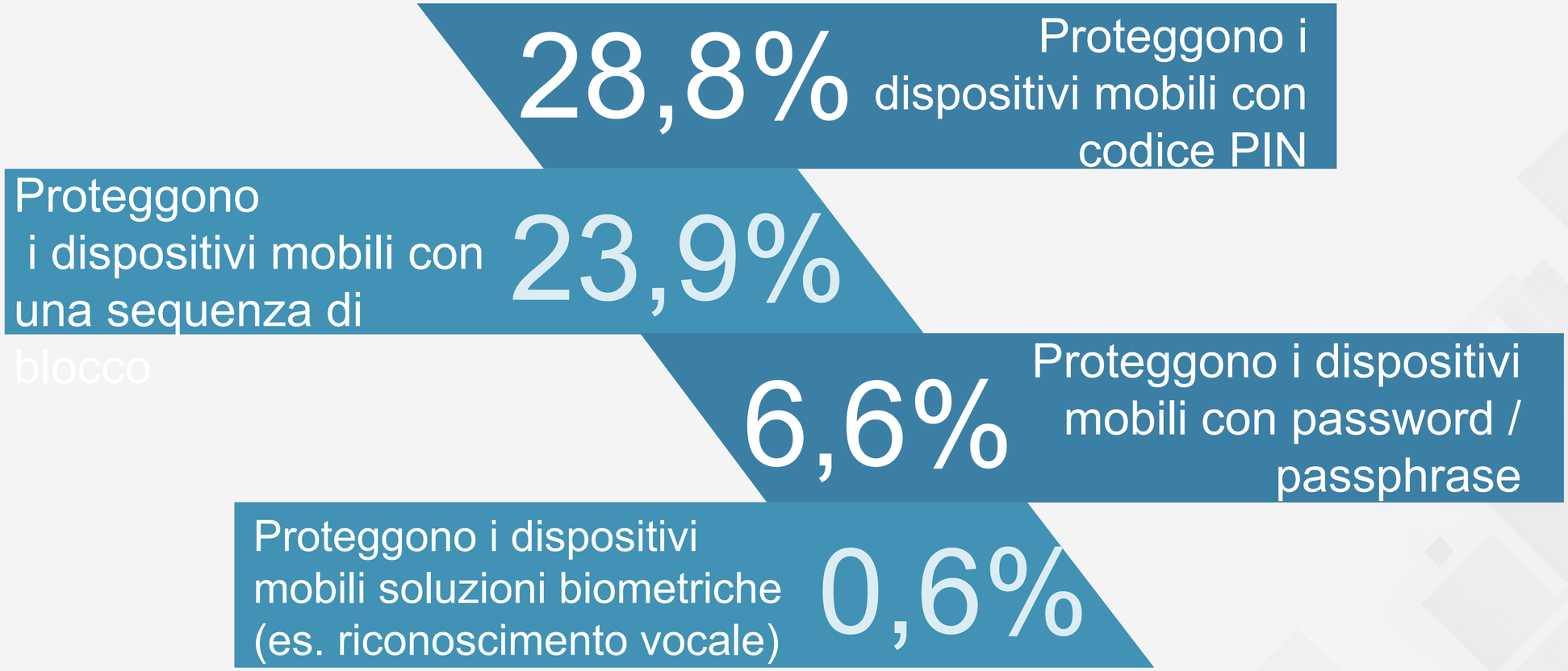
TECH AND LAW CENTER

La consapevolezza e la paura dei rischi

In che misura si sentono sicuri quando fanno queste attività con i loro dispositivi mobili

	Per nulla preoccupato	Un po' preoccupato	Abbastanza preoccupato	Molto preoccupato
Chiamate vocali	5,9	12	45,1	37
Messaggi di testo	5,1	14,2	46,2	34,5
E-mails	5,8	20,6	55	18,5
Calendario/agenda	6,6	8,8	40	44,6
Foto/video	5,2	14,6	47,2	33
Navigazione su internet	7,9	34	46	12,1
Messaging apps	8,5	26,8	48,4	16,2
Social apps	13	33,6	41,1	12,3
Mobile banking trading	41,7	31,5	18,8	7,9
Servizi Cloud	15	32	41,3	11,7
Online shopping	31,8	35,4	27,1	5,7
Videogiochi	12,9	19,6	41,9	25,6
Gambling	64,8	17,4	11,6	6,2

L'uso e la gestione della password e le tecnologie per proteggere i dispositivi mobili



Soluzioni tecniche per proteggere i dati nei dispositivi mobili

Il 20% degli studenti non conosce queste soluzioni ed un altro 20% non le utilizza. Tra i sistemi utilizzati:

	%
Lock wipe	4,0%
Remote wipe	9,0%
Find my phone	20,3%
Backup	27,7%
Encryption	4,0%
Personal firewall	5,2%
VPN	3,5%
None	12,5%
I do not know what they are	12,5%
Other	1,3%

Ultima domanda sull'autovalutazione

Come valutano la loro conoscenza sulla sicurezza dei dispositivi mobili (%)

	All'nizio del questionario (%)	Alla fine del questionario (%)
Nessuna	1,6	3,1
Poca	16,0	30,7
Abbastanza	39,3	34,4
Buono	36,6	27,4
Molto buono	6,5	4,4

Considerazioni Tecniche

Consapevolezza, conoscenza e (falsa) percezione

Quando è stato chiesto di valutare la propria conoscenza delle problematiche di sicurezza mobile, su una scala da 1 a 10, una percentuale significativamente elevata di intervistati (55 %) si sono inquadrati tra 6 e 8. Questo, tuttavia, contrasta con la percentuale media di risposte tecniche "corrette", che è stata del 29%.

Questa discrepanza tra conoscenza percepita e conoscenza effettiva emersa dalle risposte alle domande tecniche, è stata confermata dai diversi livelli di fiducia all'inizio e alla fine del sondaggio.

Infatti, dopo esser stati sottoposti alle domande di sicurezza nel sondaggio, la fiducia degli studenti universitari sul loro livello di conoscenza e' scesa dal 82% degli intervistati valutano la loro fiducia sopra 6 prima del sondaggio, al 66% alla fine.

Bisogna tuttavia tenere in considerazione la possibilita' che questi risultati siano influenzati dal cosidetto "effetto Dunning-Kruger", una distorsione cognitiva a causa della quale individui inesperti tendono a sopravvalutarsi, giudicando a torto le proprie abilità come superiori alla media.

Rischi per la Sicurezza

Rischi derivanti dalle abitudini e dai comportamenti degli studenti

Basandoci sulle risposte ricevute, abbiamo identificato tre aspetti interessanti in relazione ai rischi derivanti dal comportamento e dalle abitudini degli studenti

Problematiche generali

Come si comportano gli intervistati rispetto ai permessi richiesti dalle app ed agli aggiornamenti

7%

non aggiornano regolarmente il sistema operativo ne le applicazioni mobile

81%

aggiornano regolarmente sia il sistema operativo che le app del dispostivomobile

Nonostante ciò, la presenza sul mercato di versioni datate di sistemi operativi mobile è ancora molto alta, principalmente nei dispositivi Android

4%

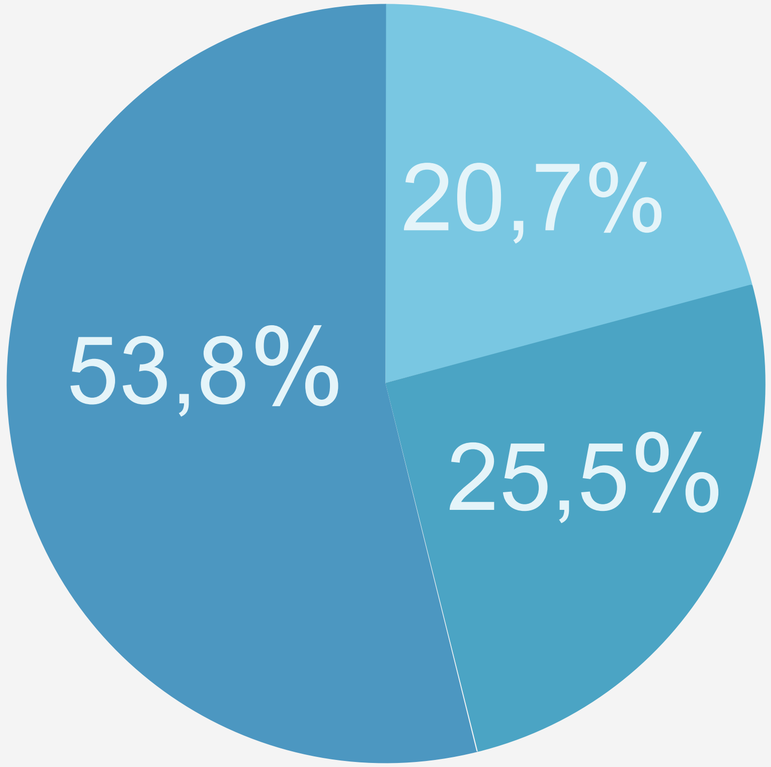
È la percentuale di dispositivi iOS che rimangono non aggiornati per più di un anno

24%

dei sistemi Android è rappresentato dalla versione Gingerbread, vecchia di 3 anni.

Problematiche generali

Come si comportano gli intervistati rispetto ai permessi richiesti dalle app ed agli aggiornamenti



Relativamente all'installazione e l'utilizzo delle app, quasi il 54% degli intervistati mai o raramente controlla i permessi richiesti dalle app. Tale comportamento è una tendenza pericolosa che deve essere affrontata: ignorare i privilegi richiesti dalle app, contribuisce ad aumentare la proliferazione di malware, dal momento che gli utenti tendono ad installare e fare clic su "SI" su qualsiasi cosa.

- Sempre
- Spesso
- Raramente/Mai

Furto d’Identità

96% memorizza la propria rubrica sui telefoni associandola a foto e video personali

effettua regolarmente il logout dopo aver ustilizzato un’app 25%

40% non utilizza alcun meccanismo di blocco per impedire l'accesso non autorizzato al dispositivo

ha affermato di non utilizzare misure di sicurezza al fine di mantenere un accesso facile e veloce al dispositivo 52%

Rischi economici e mobile malware

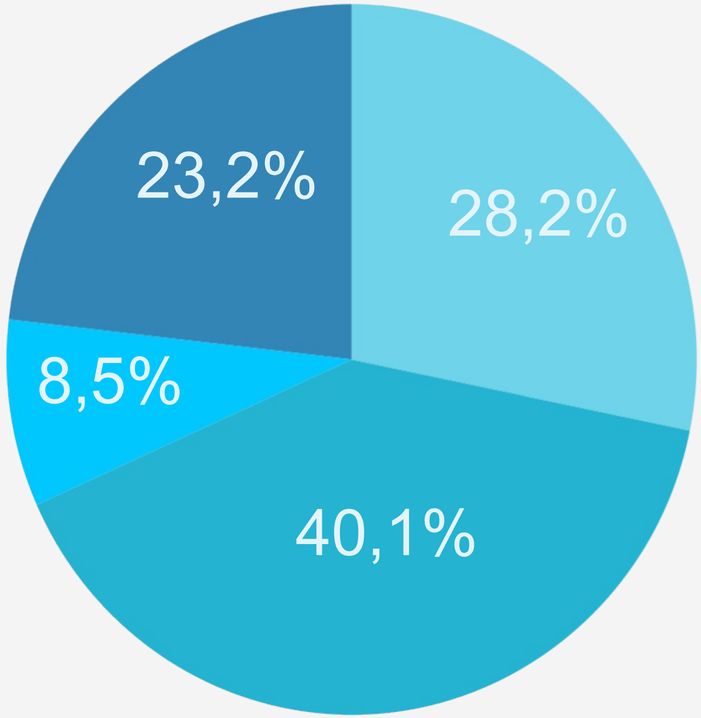
Abbiamo visto che gli utenti molto spesso non controllano i permessi richiesti dalle applicazioni. Ciò può essere dovuto al fatto che in alcune piattaforme mobile (Android, Windows Phone) i permessi sono concessi in forma "tutto o niente".

Questo è un modello pericoloso che incita le persone a trascurare i permessi, perché vogliono installare tale applicazione indipendentemente da quelli che sono i requisiti.

Questo risultato diventa più preoccupante se collegato al fatto che il 17% degli intervistati installa applicazioni da fonti "non fidate" oltre che dagli application store ufficiali di candidatura.

Questi due aspetti contribuiscono alla proliferazione di malware mobile e in particolare della categoria di frodi telefoniche, dove l'applicazione iscrive "silenziosamente" l'utente a servizi di SMS a tariffa maggiorata.

E gli sviluppatori?



Tra gli intervistati che hanno dichiarato di sviluppare applicazioni mobile (sia per hobby o profitto), solo il 28% era al corrente e seguiva le linee guida per la programmazione sicura.

- Si, le applico durante lo sviluppo delle mie applicazioni
- Si, ne ho sentito parlare ma non le conosco
- Si, le conosco ma non le applico
- No, non ne ho mai sentito parlare

Iniziative e soluzioni proposte - Produttori

Dal questionario è emerso che gli intervistati sono inclini ad aggiornare regolarmente i loro dispositivi. Possiamo dedurre da questo che sono coscienti dell'importanza degli aggiornamenti del software, ma anche che le procedure per aggiornare i dispositivi e applicazioni mobile sono notevolmente più intuitive rispetto all'ambiente "desktop".

Tuttavia, questo risultato sembra essere in contrasto con alcuni dati preoccupanti relativi al numero di dispositivi mobile che utilizzano sistemi operativi obsoleti.

La ragione di questo, possiamo affermare, è che la responsabilità probabilmente ricade su motivi quali le politiche di mercato di produttori e compagnie telefoniche e, nel caso della piattaforma Android, anche nella estrema frammentazione del mercato.

Pertanto, un ruolo fondamentale è svolto dai fornitori, che dovrebbero essere tenuti a concedere gli aggiornamenti software per i propri prodotti per un periodo di tempo più lungo.

Iniziative e soluzioni proposte – Sistemi operativi

I sistemi operativi mobile dovrebbero consentire agli utenti di installare le applicazioni senza l'obbligo di accettare tutti i permessi richiesti. Deve essere possibile per gli utenti di revocare/concedere ogni singolo permesso in qualsiasi momento, senza essere costretti a rifiutare l'intera applicazione.

Dovrebbero fornire, insieme alle funzionalità di reset del dispositivo, la possibilità di rimuovere in modo centralizzato e diretto, i dati privatidegli utenti memorizzati all'interno delle applicazioni installate.

Dovrebbero fornire soluzioni avanzate per facilitare la gestione delle password. Infatti, sebbene la maggior parte degli intervistati (85%) concordano e comprendono l'importanza di avere dei meccanismi di blocco per impedire l'accesso al dispositivo, fanno ancora fatica ad usarli.

Iniziative e soluzioni proposte - Sviluppatori

Gli sviluppatori potrebbero incentivare l'uso di password (forti), imponendo che funzionalità avanzate di alcune applicazioni vengano attivate solo se le password sono state correttamente configurate. Potrebbe essere adottato un approccio simile anche per incentivare l'uso di dispositivi che non siano stati sottoposti a jailbreaking/rooting.

Dovrebbero essere ritenuti responsabili nel caso in cui l'applicazione non implementi meccanismi di sicurezza necessarie a garantire l'adeguata gestione, memorizzazione e trasmissione dei dati degli utenti. Dovrebbero essere introdotte delle politiche, norme e leggi che ne stabiliscano la responsabilità.

Considerazioni giuridiche e definizione delle policy

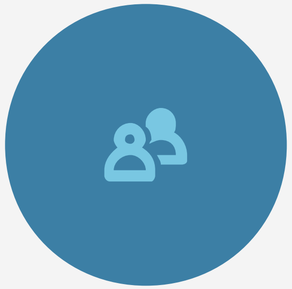
Risultati della ricerca e possibili scenari

PASSWORD

Gli studenti non prestano attenzione ai requisiti di sicurezza della password e usano spesso password prevedibili

APPLICAZIONI

Gli studenti installano software da piattaforme non autorizzate o senza dare importanza ai permessi del dispositivo



CONDIVISIONE

Il dispositivo mobile viene, anche se in percentuale ridotta, prestato a terzi o venduto senza particolari precauzioni

Risultati dell'indagine e possibili scenari

27%
salva sul proprio dispositivo, pin e password utilizzate per servizi privati

40%
non effettua il log-out dopo l'utilizzo di un servizio on-line o di una app

53%
non verifica o ,la fa molto raramente, il tipo di autorizzazioni richieste per il download di un app od altri servizi

41%
usa sul proprio dispositivo mobile sistemi Wi-Fi aperti per la connessione a Internet utilizzando tutti i tipi di funzioni

La password è … faticosa

Ne consegue che uno dei problemi più critici da affrontare nel settore IT è il fatto che gli utenti tendono a non utilizzare una password che può effettivamente essere in grado di proteggere i propri dati. La nostra ricerca, infatti, ha rivelato che il:

degli studenti intervistati non utilizza una password per proteggere il proprio dispositivo mobile **40%**

41% degli studenti intervistati, quando gli viene chiesto di cambiare la password, ne sceglie una con modifiche minime rispetto a quella precedente

degli studenti intervistati sta attualmente utilizzando "l'autenticazione a due fattori" **5%**

Furto D’indentità – Uno Scenario Legislativo frammentato

1. Manca una legislazione specifica sul furto di identità
2. Manca un sistema di reporting a livello internazionale sul furto d'identità
3. Vi è una notevole diversità sanzionatoria tra i diversi Stati maggiormente colpiti

Studio sulle misure legislative e non legislative per combattere il furto di identità e i crimine d'identità correlati: Report Finale ", RAND Europe, Giugno 2011.

Country Specific ID theft	Country Specific ID theft	Relevant provisions in criminal law?	Case law?	Specific dedicated reporting point?	Public awareness campaign?
Australia	✓	✓	✗	✓	✓
Austria	✗	✓	✗	✗	✗
Belgium	✗	✓	✓	✗	✓
Bulgaria	✗	✓	✓	✗	✗
Canada	✓	✓	✗	✗	✗
China	✗	✓	✓	✗	✗
Cyprus	✗	✓	✗	✗	✗
Czech Republic	✗	✓	✓	✗	✗
Denmark	✗	✓	✓	✗	✗
Estonia	✓	✓	✓	✗	✓
Finland	✗	✓	✓	✗	✗
France	✓	✓	✓	✗	✓
Germany	✗	✓	✓	✗	✓
Greece	✗	✓	✓	✗	✓
Hungary	✗	✓	✓	✗	✗
India	✗	✓	✓	✗	✗
Ireland	✗	✓	✓	✓	✗
Italy	✗	✓	✓	✗	✗
Japan	✗	✓	✓	✗	✓
Latvia	✗	✓	✗	✗	✗
Lithuania	✗	✓	✗	✗	✗
Luxembourg	✗	✓	✓	✗	✓
Malta	✗	✓	✓	✗	✗
The Netherlands	✗	✓	✓	✓	✓
Poland	✗	✓	✓	✗	✗
Portugal	✓	✓	✓	✗	✗
Romania	✗	✓	✓	✓	✗
Russian Federation	✗	✓	✓	✗	✗
Slovakia	✗	✓	✓	✗	✗
Slovenia	✓	✓	✓	✗	✗
Spain	✗	✓	✓	✗	✗
Sweden	✗	✓	✓	✗	✓
United Kingdom	✗	✓	✗	✓	✓
United States	✓	✓	✓	✓	✓

Furto D’ identità – Possibili soluzioni

1. Introduzione di una legislazione ad hoc

2. Rafforzamento della collaborazione tra gli organismi investigativi nazionali attraverso una rete di contatto UE

3. Sistema di reporting centralizzato su base UE

Un ottimo esempio: il progetto di CONSAP sul furto di identità in ambito Finanziario, TELCO e Assicurativo (D.Lgs 64/11)

CONSAP CONCESSIONARIA SERVIZI ASSICURATIVI PUBBLICI S.P.A.

Le recenti campagne in tema di sicurezza informatica

Il Garante delle Privacy Italiano focalizza l'attezione sul corretto utilizzo dei dispositivi mobili con la sua campagna 'Fatti smart!'

ENISA, nei prossimi mesi, organizzerà un "campionato sulla sicurezza informatica" dove gli studenti universitari competeranno sui temi della Sicurezza Informatica

enisa
European Network and Information Security Agency

Sicurezza vs. Usabilità

54,5% degli studenti vanno su siti che richiedono l'autenticazione tramite Google o Facebook.

Questo conferma in che misura l'usabilità è un fattore determinante in termini di livello di fiducia che un utente ha in un servizio online.

L'usabilità è la questione centrale per aumentare i livelli di sicurezza del dispositivo mobile

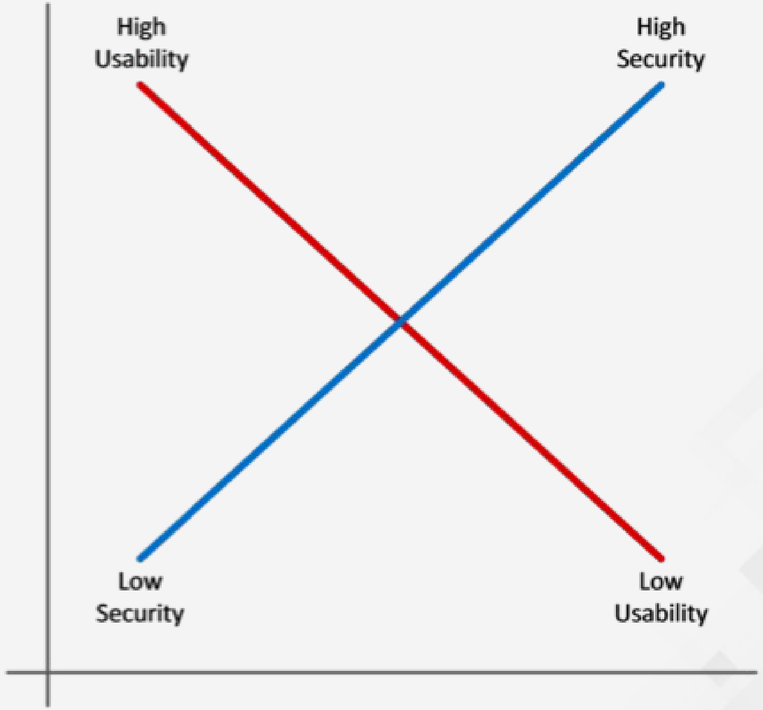


Figure 1: Security and usability tend to be inversely related

Le policy dei dispositivi mobili nelle Università

1. D. Solove: "Le scuole stanno raccogliendo e condividendo una quantità gigantesca di dati personali"
2. Non c'è una politica di sicurezza chiara per dispositivi mobili presso l'Università italiana
3. Non solo gli studenti, ma anche i Professori non sono sempre consapevoli dei rischi sulla sicurezza informatica

** D. Solove, 5 Cose che gli operatori scolastici devono sapere sulla Privacy*

In alcune università americane vengano imposti degli standard di sicurezza (e.g. HIPAA) per i device mobili di proprietà degli studenti e del personale universitario (Bring your own device - BYOD) al fine di verificare il livello di sicurezza (presenza di anti-virus, aggiornamenti del sistema operativo, presenza di sistemi di cifratura) degli stessi.

5. Conclusioni

Già nel 2002, le linee guida OCSE in materia di sicurezza dei sistemi e delle reti di informazione avevano previsto i seguenti capisaldi per la sicurezza:

Contact Us

Tech and Law
Center

www.techandlaw.net

info@techandlaw.net

twitter.com/techlawcenter

facebook.com/techandlawcenter