PRINCIPI DI SICUREZZA INFORMATICA

Come proteggere i nostri dati dalle minacce più comuni

Ing. Nicola Galotta

27/02/2016

Parleremo di …

- Sicurezza: il problema di fondo
- Da chi proteggersi
- Proteggere le informazioni significa …
- Proprietà Intellettuale
- Privacy
- Computer/Cyber Crime: Truffe e ricatti
- Dispositivi Mobili
- Potenziali vettori d'attacco
- Viaggiare

Problema di fondo

Cosa Proteggere e perché

- Quotidianamente siamo sotto attacco.

- Quali le motivazioni:
  - Appropriazione/modifica delle nostre informazioni
  - Appropriazione delle nostra identità (sostituzione di persona)
  - Appropriazione delle nostre piattaforme (spam e pubblicità)
  - Semplice divertimento distruttivo
  - Ricatto informatico (cripto virus)
  - Truffe (fishing)

- Cosa proteggere
  - Informazioni di lavoro (proprietà intellettuale)
  - Informazioni personali (privacy)
  - Noi stessi da truffe e crimini informatici

Da chi proteggersi

Hacking and Hacktivism

- Hacking è un termine ambiguo, più comunemente **percepita come parte di attività criminali**.

- Tuttavia, l'hacking è stato utilizzato per descrivere il lavoro di individui che sono stati associati con il **movimento open-source**. Molti degli sviluppi della tecnologia dell'informazione sono il risultato di ciò che è stato generalmente considerato come attività di hacking.

- Un hacker in origine era una persona che ha cercato di capire e studiare i computer a fondo.

- Presto l'hacking è stato associate a phreaking (individui che si inserivano nelle reti telefoniche per effettuare chiamate telefoniche gratuite e illegali).

Da chi proteggersi

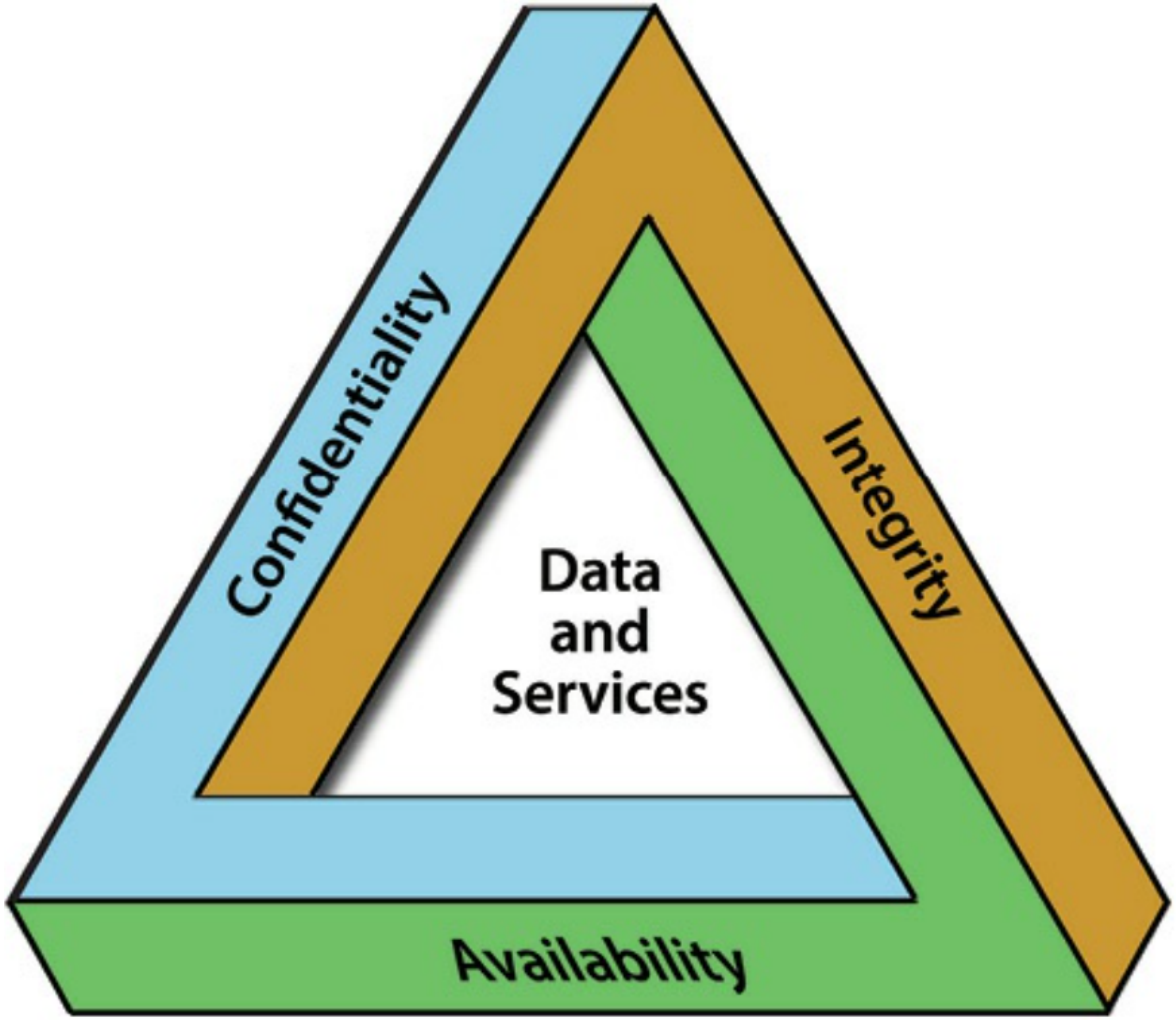
The Hacker Ethic

- L'idea di un etica hacker ha origine nelle attività degli hacker originali del MIT e Stanford negli anni 1950 e 1960.

- Stephen Levy, giornalista e autore di diversi libri su computer, la tecnologia e la privacy, ha delineato la cosiddetta etica hacker come segue:
  1. **L'accesso** ai computer deve essere **illimitato e totale**.
  2. Tutte le **informazioni** dovrebbero essere **libere**.
  3. Gli hacker devono essere **giudicati esclusivamente dalla loro abilità** di hacking, piuttosto che dalla razza, classe, età, sesso, o posizione.
  4. I computer possono essere utilizzati per **creare arte e bellezza**.
  5. I computer possono **cambiare la tua vita in meglio**.

Proteggere le informazioni significa

Garantire la CIA



Proteggere le informazioni significa

Valutare il rischio e i costi/benefici

- I rischi finanziari possono essere quantificati in molti casi, e sono generalmente utilizzati per aiutare a determinare quanto dovrebbe essere speso per il programma di recupero.
- Il rischio finanziario può essere calcolato è con la formula:

$$P * M = C$$

Probabilità di danno (P) - la possibilità che si verifichi un evento dannoso

Entità del danno (M) - la quantità di danno finanziario che si verificherebbe dovrebbe accadere un disastro.

Costo della prevenzione (C) - il prezzo di mettere in atto una contromisura prevenire i disastri colpisce. Il costo delle contromisure non dovrebbe essere superiore al costo dell'evento.

Proteggere le informazioni significa
Metodi d'identificatione

- Identification may **not be limited to human users and may include software and hardware services** that may need to access objects, modules, databases, or other applications to provide a full suite of services.
- The most common form of identification is:
  - a simple username,
  - user ID,
  - account number,
  - Personal Identification Number (PIN).

Proteggere le informazioni significa

Metodi d'identificatione

- **Identification Badges** (valido se si può garantire che ogni utente abbia sempre con se il badges).
- **User ID** (deve solo identificare non autenticare. La pwd autentica)
- **Account Number/PIN** (come user ID/passwd)
- **MAC Address** (non attendibile)
- **IP Address** (può identificare solo la zona fisica)
- **Radio Frequency Identification** (RFID) (valido se si protegge da intercettazione, traffic analysis, spoofing, DoS attack, reader integrity, privacy)
- **Email Address** (può essere usata come UserId o come parte di un processo di identificazione)

Proteggere le informazioni significa

Avere una password Strong (10 regole)

1) Utilizzare un minimo di 8 caratteri per la lunghezza della vostra password, l'ideale sarebbe una lunghezza di almeno dieci (10) o dodici (12) caratteri;

2) Utilizzare un mix di caratteri alfanumerici, ovvero tutti quei caratteri compresi fra "a" e "z" e fra "0" e "9"

3) Utilizzare sia caratteri MAIUSCOLI e minuscoli es: A/a, B/b,...Z/z che tutti quei caratteri considerati "speciali" come, "$ % & (@ # § =) , : ; - _ + ^";

4) NON Utilizzare, parole che vi identificano facilmente quali per esempio: il nome o il cognome, vostro, di vostra moglie o dei vostri cari; le date di compleanno; il numero di targa della vostra auto o il numero di cellulare, o altre banalità similari.

Proteggere le informazioni significa

Avere una password Strong (10 regole)

5) NON utilizzare, parole ovvie come ad esempio: password, pippo, pluto, 123456, qwerty, pussy, 696969, mustang, etc…

6) Cercare di NON utilizzare parole reali, eventualmente sostituite le lettere con il loro"uguale" numerico, come ad esempio la parola "pessimista" potrebbe diventare "p355im1stA" ancora meglio se si aggiungono caratteri speciali "P3S5!m1ST@"

7) Un altro metodo per creare una password facilmente ricordabile, è quello di pensare per esempio al film preferito ed utilizzarne una frase famosa, come: "domani è un altro giorno e si vedrà" prendendo le lettere iniziali e/o finali di ogni singola parola, per costruire la password es:"DièUnaOGesiVà" o ancora meglio "D13'Un@OGe5iV@'"

Proteggere le informazioni significa

Avere una password Strong (10 regole)

8) Cambiare regolarmente la password per lo meno quelle di importanza strategica, il cambio andrebbe effettuato, almeno una volta ogni 2 o tre mesi.

9) ASSOLUTAMENTE EVITARE di utilizzare sempre la medesima password per tutte le innumerevoli richieste di accesso, sia esse al lavoro che a casa.

10) Se avete l'abitudine di tenere una traccia scritta delle vostre password, assicuratevi che tale traccia sia conservata lontano da occhi indiscreti e al sicuro. Evitate di scrivere le password sul cellulare o nel classico foglietto sulla scrivania dell'ufficio, o all'interno del portafogli.

Proprietà Intellettuale

- Le leggi sulla proprietà intellettuale sono pensate per **proteggere gli elementi materiali e immateriali e la loro proprietà**.

- Anche se ci sono diverse motivazioni che stanno dietro la protezione per questo tipo di proprietà, l'obiettivo generale del diritto di proprietà intellettuale è quello di proteggere la proprietà **da coloro che desiderano copiare o usarlo, senza il dovuto compenso all'inventore o al creatore**.

- L'idea è che **la copia o l'utilizzo idee di qualcun altro comporta molto meno lavoro** rispetto a quanto richiesto per lo sviluppo originale.

Proprietà Intellettuale

- Secondo l'Organizzazione mondiale della proprietà intellettuale (OMPI), la proprietà intellettuale si divide in due categorie:

  - **proprietà industriale**, che include invenzioni (brevetti), marchi, disegni industriali, e delle indicazioni geografiche di provenienza;

  - **diritti d'autore (copyright)**, che comprende opere letterarie e artistiche, come romanzi, poesie e opere teatrali, film, opere musicali, opere artistiche come disegni, dipinti, fotografie e sculture e progetti architettonici.

- Il problema del **Trans-Border data flow** e delle leggi locali (dropbox, google drive, …).

Privacy

- Con la proliferazione della tecnologia e la crescente consapevolezza che la maggior parte del**le nostre informazioni personali (PII) è memorizzato in linea o per via elettronica,** in qualche modo, forma o forma, vi è una crescente pressione per proteggere informazioni.

- Quasi ogni mese, ci sono notizie sulla stampa di tutto il mondo di database compromessi, file che vengono persi, e **attacchi contro le imprese ed i sistemi che ospitano, informazioni private personali**.

- Questo ha suscitato **preoccupazioni per la corretta raccolta, uso, conservazione e distruzione delle informazioni di carattere personale o riservato**.

Privacy

- Questa preoccupazione ha spinto la **creazione di norme** destinate a favorire l'uso responsabile e gestione delle informazioni personali.

- Indipendentemente dal metodo, l'**obiettivo generale** è quello di **proteggere le informazioni personali** di un cittadino, e allo stesso tempo **garantire il bilanciamento** per le esigenze di business o di ricerca che hanno bisogno di **raccogliere e utilizzare** queste informazioni in modo appropriato.

- Purtroppo, **non esiste un diritto internazionale della privacy**, con conseguente in un mosaico di leggi e regolamenti. Alcuni paesi hanno progressivamente trattato la privacy e le informazioni personali, mentre altri devono ancora agire in questo settore.

Privacy

- Tenuto conto del fatto che **Internet ha creato una comunità globale**, le nostre informazioni e le transazioni commerciali e le operazioni possono attraversare diversi **confini e giurisdizioni diverse** - ciascuna con le proprie preoccupazioni sovrane, le norme sociali, e le leggi.

- Pertanto, **è prudente avere una conoscenza di base dei principi di privacy** e delle linee guida e tiene aggiornato con il paesaggio che cambia di norme sulla privacy che possono influenzare le imprese così come le informazioni personali.

Computer/Cyber Crime

Truffe e ricatti

- Con la proliferazione di virus, spyware, schemi di phishing e frodi, e l'**attività di hacking da ogni posizione nel mondo**, la criminalità informatica e la sicurezza sono certamente argomenti di interesse quando si parla di etica del computer.

- Oltre agli estranei (**o hacker**), molti crimini informatici, come appropriazione indebita o l'impianto di bombe logiche, sono commessi da **personale di fiducia** che hanno l'autorizzazione ad utilizzare i sistemi informatici aziendali.

Computer/Cyber Crime: Truffe e ricatti

Cryptolocker ransomware

Computer/Cyber Crime: Truffe e ricatti

Cryptolocker ransomware

- **Cryptolocker ransomware** - Si diffonde **via e-mail** e si propaga rapidamente.
- Il virus **cripta vari tipi di file** e quindi viene visualizzata una finestra pop-up sui computer delle vittime che dichiara i loro dati sono stati crittografati.
- L'unico modo per farlo tornare è quello di inviare un pagamento monetario specificato l'autore.
- Questo ransomware informa la vittima entro quanto tempo pagare attraverso la visualizzazione di un **conto alla rovescia**.
- Se le vittime non pagano in tempo, perdono i propri dati in modo permanente criptati e resi inutilizzabili.
- Gli autori chiedono un pagamento $ 300 a $ 700.

Computer/Cyber Crime: Truffe e ricatti

Child Pornography Scareware

Computer/Cyber Crime: Truffe e ricatti

Child Pornography Scareware

- **Child Pornography Scareware** - Questo scareware viene trasmesso quando gli utenti di computer **visitano un sito infetto**.
- Il computer vittima si blocca e viene visualizzato un **avviso che l'utente ha violato la legge**.
- La pornografia infantile è infatti integrata in un banner che appare sullo schermo delle vittime o appare nel browser tramite una re-indirizzamento automatico a un sito web di pornografia infantile.
- Il scareware è utilizzato come **tecnica di estorsione con la minaccia penale** per la visita o la visualizzazione di queste immagini.
- La vittima è inoltre informato che lui o lei è stato registrato con audio, video e altri dispositivi.
- L'unico modo per sbloccare il computer è quello di pagare la multa, che è di solito tra $ 300 e $ 5.000.

Computer/Cyber Crime: Truffe e ricatti

Citadel Ransomware

Computer/Cyber Crime: Truffe e ricatti

Citadel Ransomware

- **Citadel Ransomware** - Il ransomware Cittadella, chiamato Reveton, mostra un avviso sul computer delle vittime sostenendo che il loro **computer è stato utilizzato per attività illegali**, come ad esempio il download di software protetto da copyright o materiale pedopornografico.
- Per aumentare l'illusione di essere osservati dalle forze dell'ordine, lo schermo visualizza anche l'indirizzo IP della vittima, e alcune vittime anche relazione sull'attività loro webcam.
- Alle vittime viene intimato di **pagare una multa** al Dipartimento di giustizia **per sbloccare il loro computer**.
- Oltre a installare il ransomware, il malware Cittadella continua a funzionare sul computer infetto per **raccogliere i dati sensibili che potrebbero essere utilizzati per commettere una serie di frodi finanziarie**.

Computer/Cyber Crime

Fake or Rogue Anti-Virus Software

Computer/Cyber Crime: Truffe e ricatti

Fake or Rogue Anti-Virus Software

- **Fake or Rogue Anti-Virus Software** - In questo schema, le vittime vengono indotte ad acquistare un software anti-virus che dovrebbe presumibilmente **rimuovere i virus dai loro computer**.
- Una finestra pop-up appare che informa gli utenti che i loro computer sono pieni di virus e devono essere puliti.
- Il messaggio pop-up ha un pulsante le vittime possono fare clic per l'acquisto di software anti-virus che presumibilmente può immediatamente sbarazzarsi di questi virus.
- **Se le vittime cliccano sul pop-up per l'acquisto del software anti-virus, vengono infettate dal malware**. In alcuni casi, le vittime sono state infettate a prescindere cliccando sulla casella pop-up.

Computer/Cyber Crime: Truffe e ricatti

Come evitare di diventare vittime

- Diffidare di chiamate indesiderate telefonate, visite, o messaggi e-mail da persone che chiedono sui dipendenti o altre informazioni interne.

- Se un individuo sconosciuto sostiene di appartenere a un'organizzazione legittima, provare a verificare la sua identità direttamente con l'azienda.

- Non fornire informazioni personali o informazioni sulla vostra organizzazione, compresa la sua struttura o reti, a meno che non si è certi di autorità di una persona di avere le informazioni.

- Non rivelare informazioni personali o finanziarie in email, e non rispondere alle email sollecitazioni per queste informazioni.

Computer/Cyber Crime: Truffe e ricatti

Come evitare di diventare vittime

- Non inviare informazioni sensibili su Internet prima di controllare la sicurezza di un sito web.

- Prestare attenzione alla URL di un sito web. Siti web maligni possono sembrare identici a un sito legittimo, ma l'URL può utilizzare una variazione di ortografia o un dominio diverso (ad esempio, .com .net vs).

- Se non siete sicuri se una mail di richiesta è legittima, provare a verificare contattando direttamente l'azienda.

- Non utilizzare le informazioni di contatto fornite su un sito web collegato alla richiesta; invece, per verificare utilizzate le informazioni sui contatti presenti in fattura o altrove.

Computer/Cyber Crime: Truffe e ricatti

Come evitare di diventare vittime

- Informazioni su attacchi di phishing noti sono disponile anche on-line da gruppi come il Gruppo Anti-Phishing Working (http://www.antiphishing.org).

- Installazione e manutenzione di software, firewall e filtri di posta elettronica anti-virus per ridurre una parte di questo traffico.

- Approfittate di tutte le funzioni anti-phishing offerti dal tuo client di posta elettronica e il browser Web.

Dispositivi Mobili

- Sono prodotti variano da **sofisticati** telefoni cellulari, come ad esempio telefoni cellulari di quarta generazione (4G), a "ultrabooks" full-optional e tablet.

- Questi dispositivi possono ora **gestire le informazioni personali**, come ad esempio i contatti, gli appuntamenti, e to-do list.

- I dispositivi mobili attuali e telefoni cellulari si connettono a Internet, funzionano come **dispositivi di sistema di posizionamento globale** (GPS), ed eseguire software multimediale.

- Essi possono anche sostenere una **rete senza fili** Bluetooth e reti WAN wireless (WAN).

Dispositivi Mobili

- Hanno slot per schede di memoria che **accettano supporti flash** che può servire come archiviazione aggiuntivo per i file e le applicazioni.

- La maggior parte dei tutti i dispositivi **forniscono supporto audio e video**, che incorporano lettori MP3, un microfono, un altoparlante, jack per le cuffie e con un built-in fotocamera digitale.

- **funzioni di sicurezza integrate**, come un lettore biometrico di impronte digitali possono anche essere inclusi.

Dispositivi Mobili

- In molti casi, i **servizi di sicurezza sono stati sacrificati** per fornire l'interazione dell'utente ricca quando la potenza di elaborazione è molto limitata.

- La loro mobilità ha resi **un primo vettore per la perdita di dati** perché possono essere utilizzati per trasmettere e memorizzare le informazioni in modi che possono essere difficili da controllare.

IPAD/IPOD/IPHONE SPECIFIC BEST PRACTICES

- Use of configuration templates to set up the device on the enterprise network and to enforce suggested policies on the device, including:
  - Use of a passcode (strength dependent on the potential data the device may contain)
  - Allow device wipe if 10 failed passcode attempts
  - Use of Cisco AnyConnect VPN – Available in the Apple App Store
  - Encryption of device configuration profile
  - Forced encryption of device backups
  - If multiple users will be accessing the device, the native mail program should not be used to protect the primary user's email account.
  - If the device is no longer in use, ensure that all of the data on it is wiped, and it is disposed of properly.

Potential attack vectors

- SMS
  - SMS messages on the device can be forwarded to the attacker, or the attacker can search them for valuable information.
  - Many commerce sites, including financial institutions, communicate one time passwords or credential information through SMS as an out-of-band channel.
  - SMS can be utilized as a means to perform transactions that can lead to an attacker being able to perform unauthorized transactions from the device.
- Email
  - If the device is being used to send or retrieve email messages, the messages can be forwarded or searched by an attacker. This includes private as well as corporate email messages.
  - Email messages could likely contain sensitive company information as well as other private information such as credentials from password reset links.

Potential attack vectors

- Phone
  - Low-level access to the hardware of mobile devices through mobile operating systems can provide an attacker the ability to record or listen to voice conversations.
- Video/Photo
  - Low-level access to the hardware of mobile devices through mobile operating systems can provide an attacker the ability to activate the internal camera to record video or take photos from the phone to provide detailed views of the device's surroundings.
- Social Networking
  - Social networking applications running on a smartphone can be utilized to propagate malware through the trust of the users associated with the compromised account.
  - Impersonation carried out as the associated account can allow the retrieval of personal information about the users and their social contacts.

Potential attack vectors

- Location Information
  - Most mobile phones provide location information (for example, using built-in GPS or GSM antenna info), so it may be possible for an attacker to query this information on the device to determine where the device is located.
- Voice Recording
  - Low-level access to the hardware of mobile devices through mobile operating systems can provide an attacker the ability to activate the internal microphone to record any sound or voice close to the mobile phone, including phone calls.
- Documents
  - The attacker can retrieve documents stored on the device, including attachments from emails.
    Document types can include PDF files, Microsoft Office files, credentials, encryption certificates, internal videos or internal e-books, among others.
- Credentials
  - Cached credentials may be stored insecurely inside third-party applications.

Risks from Mobile Workers

- The list below categorizes some of the potential attack vectors for mobile devices:
  - **Wi-fi**
  - **Bluetooth**
  - **Infra-red**
  - **USB**
  - SMS
  - Email client
  - Web browser
  - Third-party applications
  - "Jail-broken" phones
  - Operating system vulnerabilities
  - Physical access

Travel
YOU SHOULD KNOW

- In most countries, you have no expectation of privacy in Internet cafes, hotels, offices, or public places. Hotel business centers and phone networks are regularly monitored in many countries.

- All information you send electronically – by fax machine, personal digital assistant (PDA), computer, or telephone – can be intercepted. Wireless devices are especially vulnerable.

- Security services and criminals can track your movements using your mobile phone or PDA and can turn on the microphone in your device even when you think it's off. To prevent this, remove the battery.

Travel
YOU SHOULD KNOW

- Security services and criminals can also insert malicious software into your device through any connection they control. They can also do it wirelessly if your device is enabled for wireless. When you connect to your home server, the "malware" can migrate to your business, agency, or home system, can inventory your system, and can send information back to the security service or potential malicious actor.

- Malware can also be transferred to your device through thumb drives (USB sticks), computer disks, and other "gifts."

- Transmitting sensitive government, personal, or proprietary information from abroad is therefore risky.

Travel
YOU SHOULD KNOW

- Corporate and government officials are most at risk, but do not assume you are too insignificant to be targeted.

- Foreign security services and criminals are adept at "phishing" – that is, pretending to be someone you trust in order to obtain personal or sensitive information.

- If a customs official demands to examine your device or if your hotel room is searched while the device is in the room and you are not, you should assume the device's hard drive has been copied.

Travel

BEFORE YOU TRAVEL

- If you can do without the device, don't take it.
- Do not take information you do not need, including sensitive contact information.
- Consider the consequences if your information were stolen by a foreign government or competitor.
- Backup all information you take; leave the backed-up data at home.
- If feasible, use a different mobile phone or PDA from your usual one and remove the battery when not in use.
- In any case, have the device examined by your agency or company when you return.
- Seek official cybersecurity alerts: http://www.viaggiaresicuri.it (sito della Franesina).

Travel
WHILE YOU'RE AWAY

- Avoid transporting devices in checked baggage.
- Use digital signature and encryption capabilities when possible.
- Do not leave electronic devices unattended.
- If you have to stow them, remove the battery and SIM card and keep them with you.
- Do not use thumb drives given to you; they may be compromised.
- Do not use your own thumb drive in a foreign computer for the same reason. If you're required to do it anyway, assume you have been compromised; have your device cleaned as soon as you can.

Travel
WHILE YOU'RE AWAY

- Shield passwords from view. Do not use the "remember me" feature on many websites; retype the password every time.
- Be aware of who is looking at your screen, especially in public areas.
- Terminate connections when you're not using them.
- Clear your browser after each use: Delete history files, caches, cookies, URL, and temporary Internet files.
- Do not open emails or attachments from unknown sources.

Travel
WHILE YOU'RE AWAY

- Do not click on links in emails. Empty your "trash" and "recent" folders after every use.
- Avoid Wi-Fi networks if you can. In some countries, they are controlled by security services; in all cases, they are insecure.
- If your device or information is stolen, report it immediately to your home organization and the local U.S. embassy or consulate.

Travel
WHEN YOU RETURN

- Change your password.
- Have your company or agency examine the device for the presence of malicious software.
- For general travel alerts and information, see:
  - http://travel.state.gov/content/passports/english/alertswarnings.html
  - http://www.viaggiaresicuri.it (sito della Franesina)

Grazie per l'attenzione

www.circoloingegneri.it
info@circoloingegneri.it

www.agcitalia.com
info@agcitalia.com