IT Security Specialized Level

Ing. Gianpiero Ciacci

Release 11 aprile 2017

IT Security

ATENEO INTERNAZIONALE
Università per Stranieri di Siena

Riepilogo argomenti

- **1 - Concetti di sicurezza**
- **2 - Malware**
- **3 - Sicurezza in rete**
- **4 - Controllo di accesso**
- **5 - Uso sicuro del web**
- **6 - Comunicazioni**
- **7 - Gestione sicura dei dati**

http://www.ecdl.it/documents/100682/141605/IT_Security_Syllabus_IT_2.0_IT.pdf/

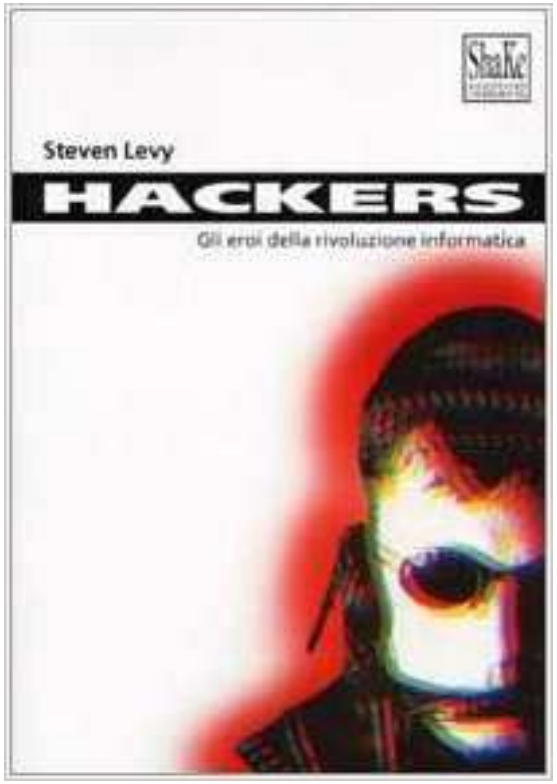
1 – Concetti di sicurezza

ATENEO INTERNAZIONALE
Università per Stranieri di Siena

1.1 – Minacce ai dati

- Dati e informazioni
- Crimine informatico
- Hacker, cracker, lamer
- Hacker etico (white hat)
- Minacce dolose e accidentali ai dati provocate da singoli individui, fornitori di servizi, organizzazioni esterne.
- Minacce ai dati provocate da circostanze straordinarie, quali fuoco, inondazioni, guerre, terremoti.
- Minacce ai dati provocate dall'uso del cloud computing, quali controllo sui dati, potenziale perdita di riservatezza (privacy).

Letture consigliate



Guida galattica per autostoppisti (2005)

Hackers (1995)

1 – Concetti di sicurezza

1.2 - Valore delle informazioni

- Sicurezza delle informazioni: *confidenzialità*, *integrità*, *disponibilità*.
- Proteggere le informazioni personali: evitare il furto di identità o le frodi, mantenere la riservatezza.
- Proteggere informazioni di lavoro su computer e dispositivi mobili: evitare furti, utilizzi fraudolenti, perdite accidentali di dati, sabotaggi.
- Principi comuni per la protezione conservazione e controllo dei dati e della riservatezza, quali: trasparenza, scopi legittimi, proporzionalità delle misure in rapporto ai danni.
- "soggetti dei dati" e "controllori dei dati", applicazione dei principi di protezione, conservazione e controllo dei dati e della riservatezza
- Linee guida e politiche per l'uso dell'ICT

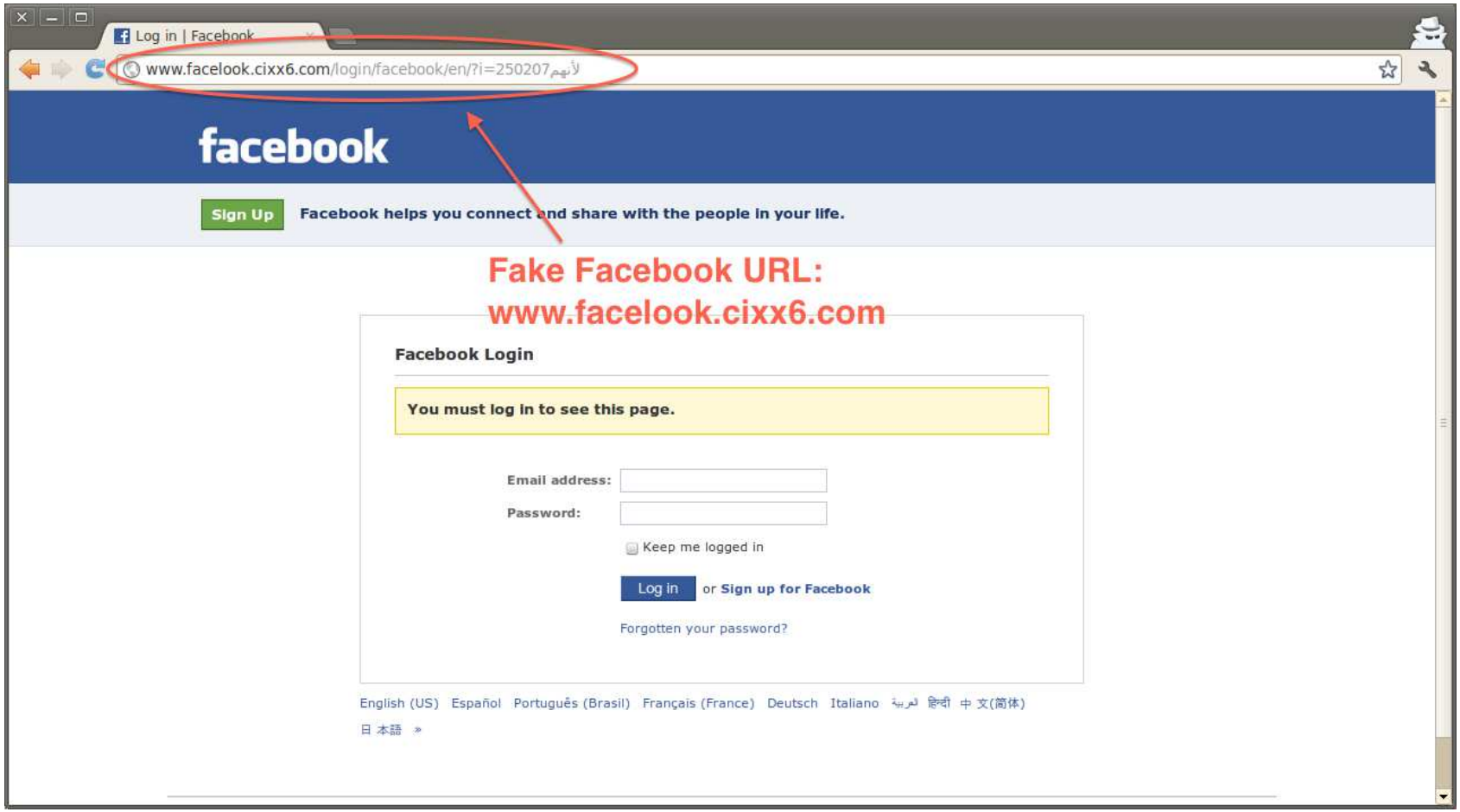
1 – Concetti di sicurezza

1.3 - Sicurezza personale

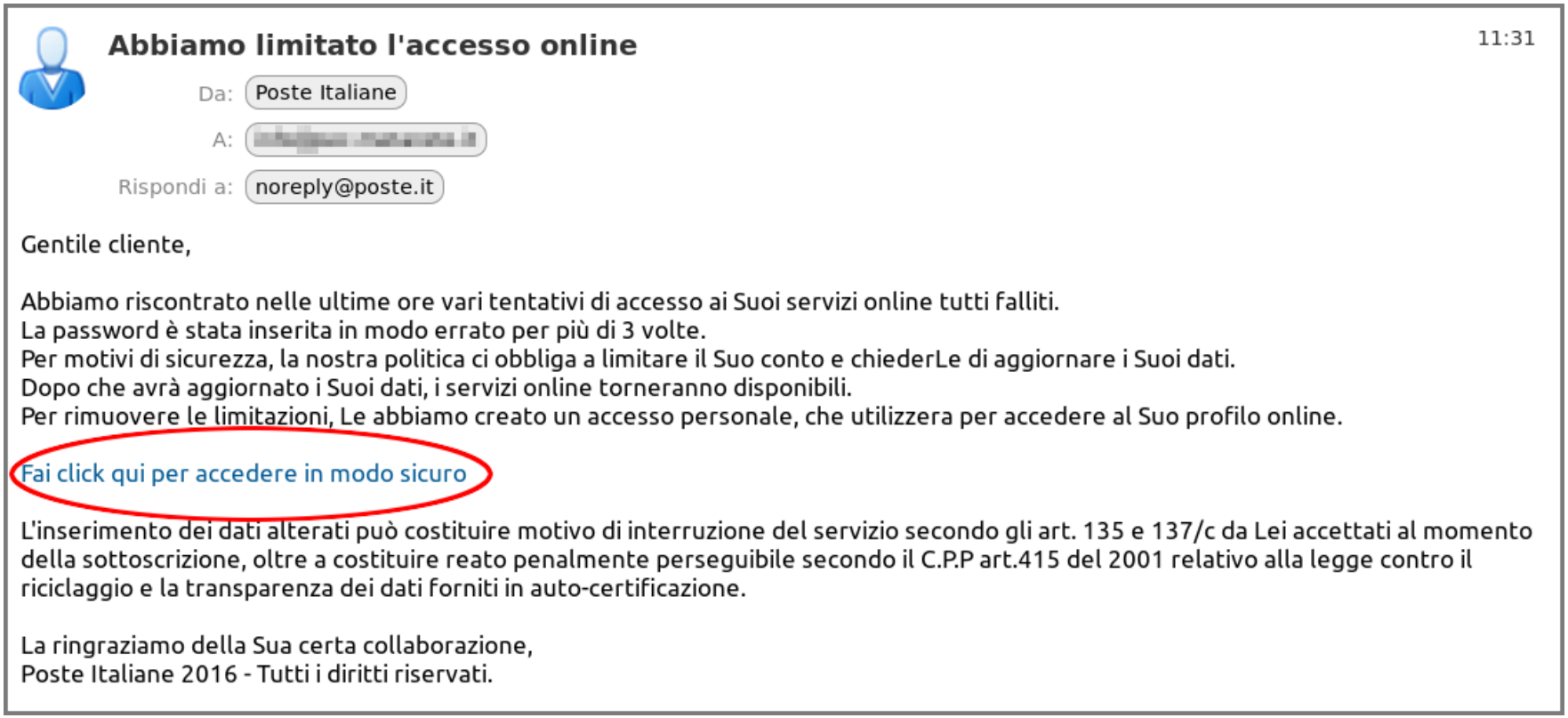
- "ingegneria sociale": accesso non autorizzato a sistemi informatici, raccolta non autorizzata di informazioni, frodi.
- Metodi: chiamate telefoniche, phishing, shoulder surfing
- "furto di identità": implicazioni personali, finanziarie, lavorative, legali.
- Metodi: acquisire informazioni a partire da oggetti e informazioni scartati (information diving); uso di dispositivi fraudolenti di lettura (skimming); inventare uno scenario pretestuoso (pretexting).

Prova a prendermi (2002)

Phishing – URL contraffatta



Phishing email



Abbiamo limitato l'accesso online 11:31

Da: Poste Italiane

A: [redacted]

Rispondi a: noreply@poste.it

Gentile cliente,

Abbiamo riscontrato nelle ultime ore vari tentativi di accesso ai Suoi servizi online tutti falliti.
La password è stata inserita in modo errato per più di 3 volte.
Per motivi di sicurezza, la nostra politica ci obbliga a limitare il Suo conto e chiederLe di aggiornare i Suoi dati.
Dopo che avrà aggiornato i Suoi dati, i servizi online torneranno disponibili.
Per rimuovere le limitazioni, Le abbiamo creato un accesso personale, che utilizzera per accedere al Suo profilo online.

Fai click qui per accedere in modo sicuro

L'inserimento dei dati alterati può costituire motivo di interruzione del servizio secondo gli art. 135 e 137/c da Lei accettati al momento della sottoscrizione, oltre a costituire reato penalmente perseguibile secondo il C.P.P art.415 del 2001 relativo alla legge contro il riciclaggio e la transparenza dei dati forniti in auto-certificazione.

La ringraziamo della Sua certa collaborazione,
Poste Italiane 2016 - Tutti i diritti riservati.

Bancomat clonati

1 – Concetti di sicurezza

ATENEO INTERNAZIONALE
Università per Stranieri di Siena

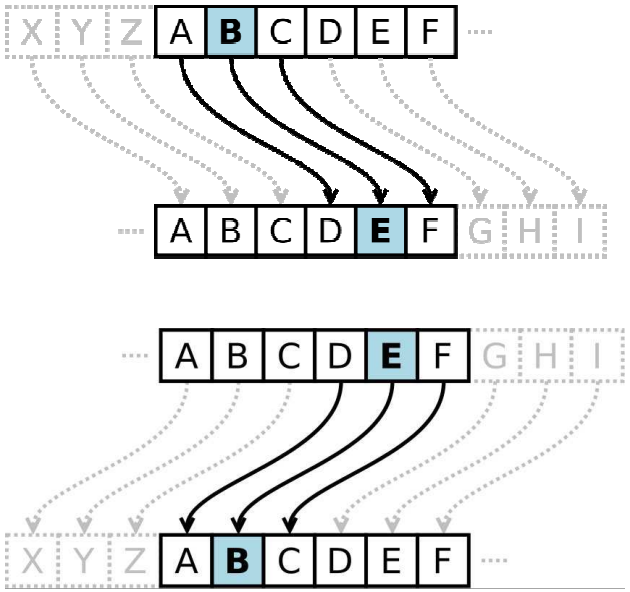
1.4 - Sicurezza dei file

- Impostazioni di sicurezza relative alle macro.
- Cifratura. Non divulgare o perdere la password, la chiave o il certificato di cifratura.
- Cifrare un file, una cartella, una unità disco.
- Impostare una password per file.

Scitala spartana

- Crittografia per trasposizione
- Striscia di pergamena avvolta attorno ad una bacchetta
- Plutarco, *Vita di Lisandro*

Cifrario di Cesare



Cifratura

BENVENUTI

+4

FIRZIRYXM

Decifratura

-4

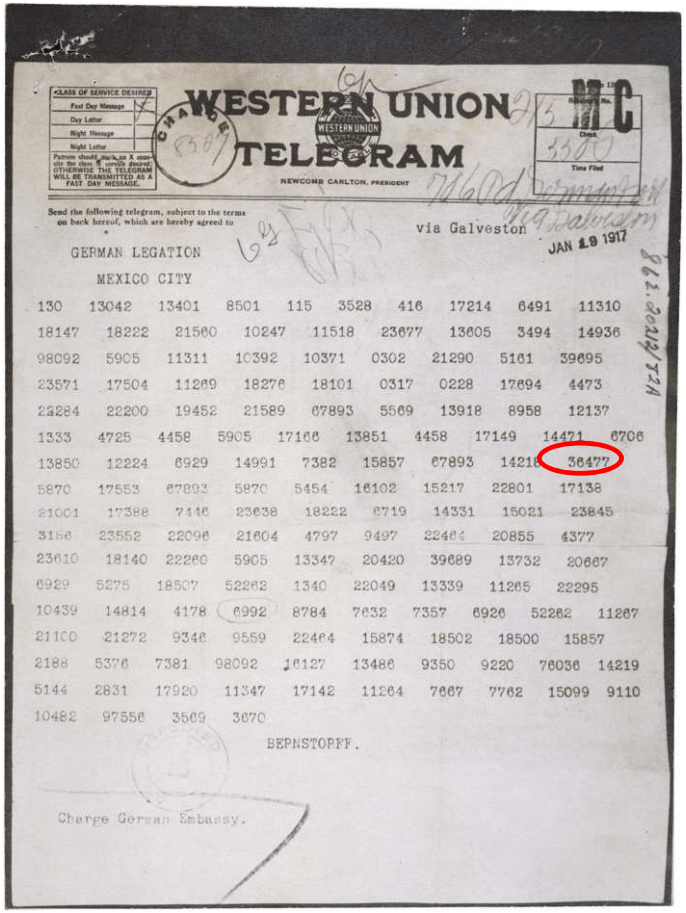
BENVENUTI

Cifrario di Vigenère (1586)

```
Testo chiaro  - RAPPORTOIMMEDIATO
Verme         - VERMEVERMEVERMEVE
Testo cifrato - MEGBSMXFUQHIUUEOS
```

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Telegramma Zimmermann (1917)



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

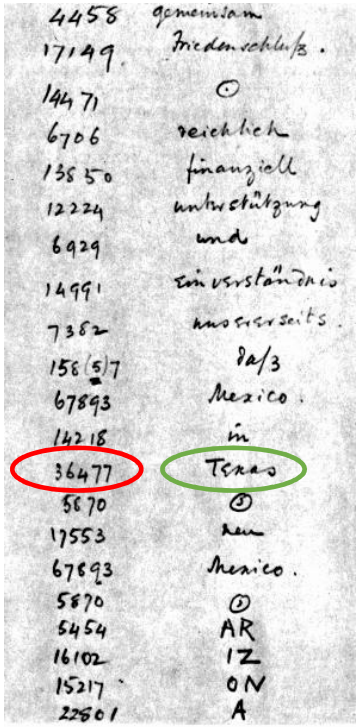
JAN 19 1917

GERMAN LEGATION
MEXICO CITY

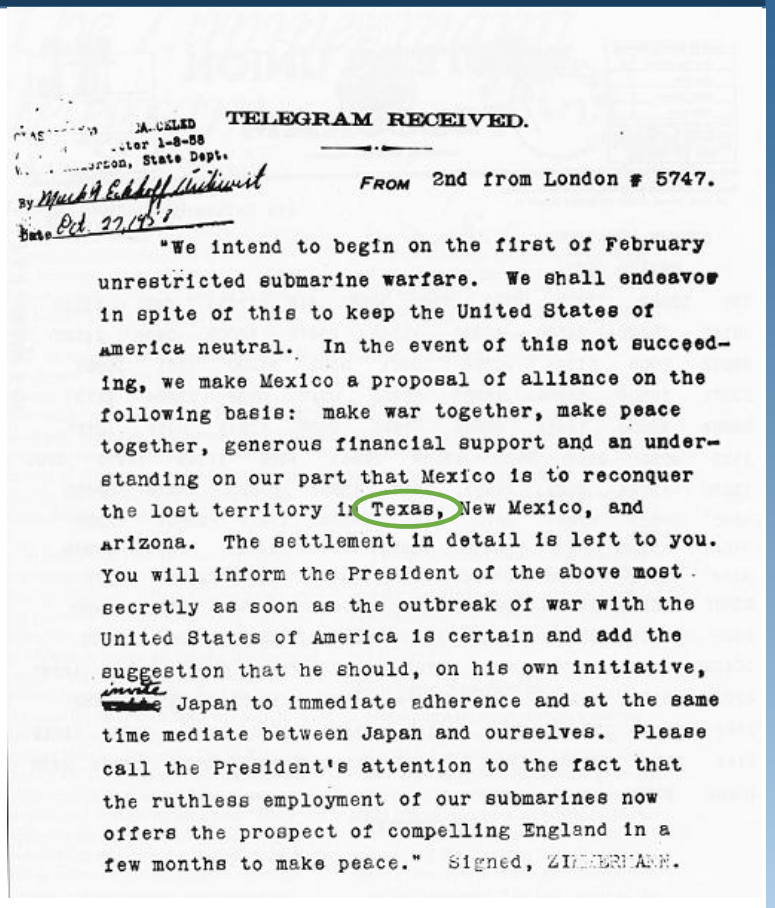
130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTORFF.

Charge German Embassy.



4458 geneinsam
17149 Friedenschluß.
14471 ⊙
6706 reichlich
13850 finanziell
12224 unterstützung
6929 und
14991 einverständnis
7382 unserseits.
15857 da/3
67893 Mexico.
14218 in
36477 Texas
5870 ①
17553 neu
67893 Mexico.
5870 ①
5454 AR
16102 IZ
15217 ON
22801 A



TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

https://it.wikipedia.org/wiki/Telegramma_Zimmermann

Windtalkers (2002)

Macchina Enigma

The imitation game (2014)

Funzionamento della macchina Enigma

Cifrario di Vernam

- Unico cifrario con la sicurezza dimostrata matematicamente (Shannon, 1949)
- Chiavi monouso di lunghezza pari al messaggio da cifrare (spie nella guerra fredda con taccuini con una lunga chiave per ogni pagina, da strappare dopo l'uso)

```
CIHJT UUHML FRUGC ZIBGD BQPNI PDNJG LPLLP YJYXM
DCXAC JSJUK BIOYT MWQPX DLIRC BEXYK VKIMB TYIPE
UOLYQ OKOXH PIJKY DRDBC GEFZG UACKD RARCD HBYRI
DZJYO YKAIE LIUYW DFOHU IOHZV SRNDD KPSSO JMPQT
MHQHL OHQQD SMHNP HHOHQ GXRPJ XBXIP LLZAA VCMOG
AWSSZ YMFNI ATMON IXPBY FOZLE CVYSJ XZGPU CTFQY
HOVHU OCJGU QMWQV OIGOR BFHIZ TYFDB VBRMN XNLZC
```

Algoritmi a chiave simmetrica (o privata)

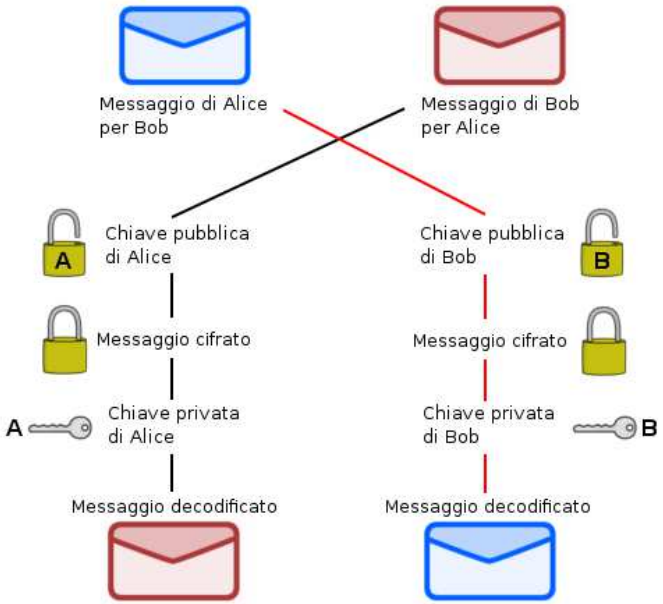
- Mittente e destinatario condividono la stessa chiave per cifrare/decifrare il messaggio e deve esistere un sistema sicuro per scambiarsi la chiave segreta
- Esempio di algoritmi: DES, 3DES, AES

$$S(P,k) = C \qquad D(C,k) = P$$

- S = algoritmo di crittazione a chiave simmetrica
- D = algoritmo di decrittazione a chiave simmetrica
- P = Plain text message
- k = key
- C = Cypher text message

Algoritmi a chiave asimmetrica (o pubblica)

- La chiave pubblica viene usata da chiunque per cifrare il messaggio, ma solo il destinatario con la corrispondente chiave privata può decifrarlo
- Esempio di algoritmo: RSA
- Basata su difficoltà della fattorizzazione
- Dati A e B di centinaia di cifre, ottenere C=A*B è facile e veloce, ma partire da C per ottenere A e B richiede enorme potenza di calcolo e tempo



2 - Malware

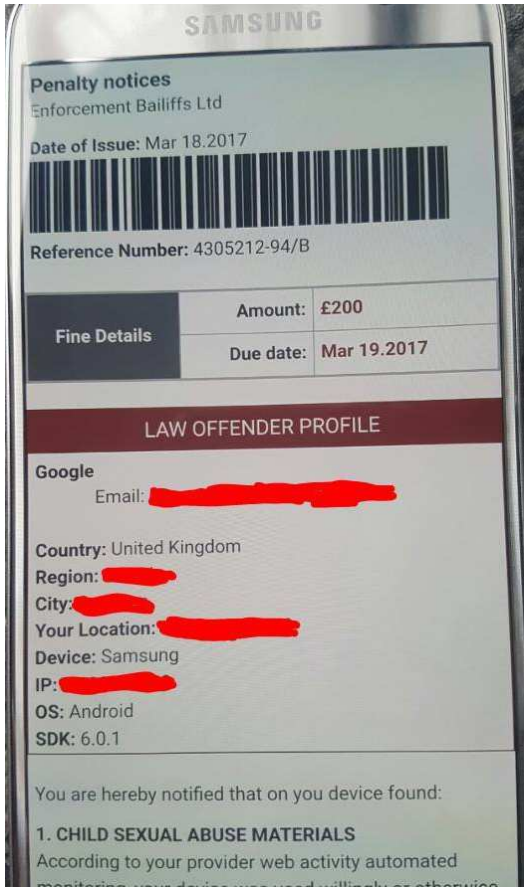
ATENEO INTERNAZIONALE
Università per Stranieri di Siena

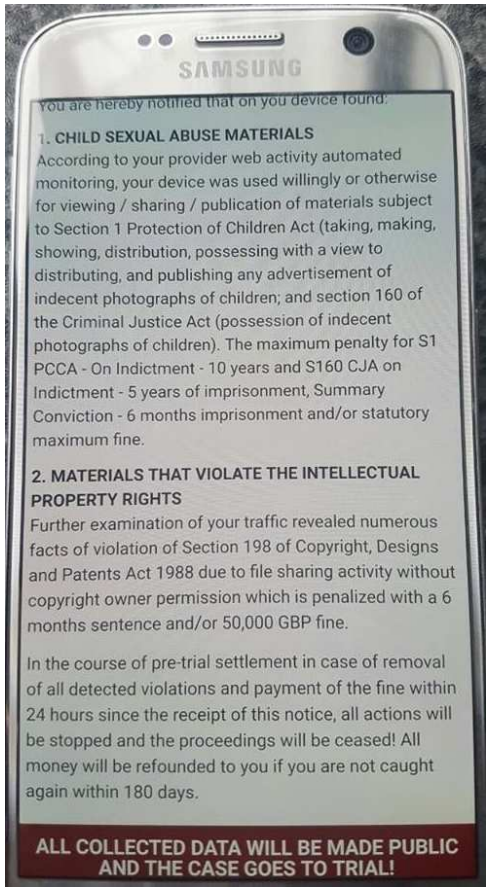
2.1 - Tipi e metodi

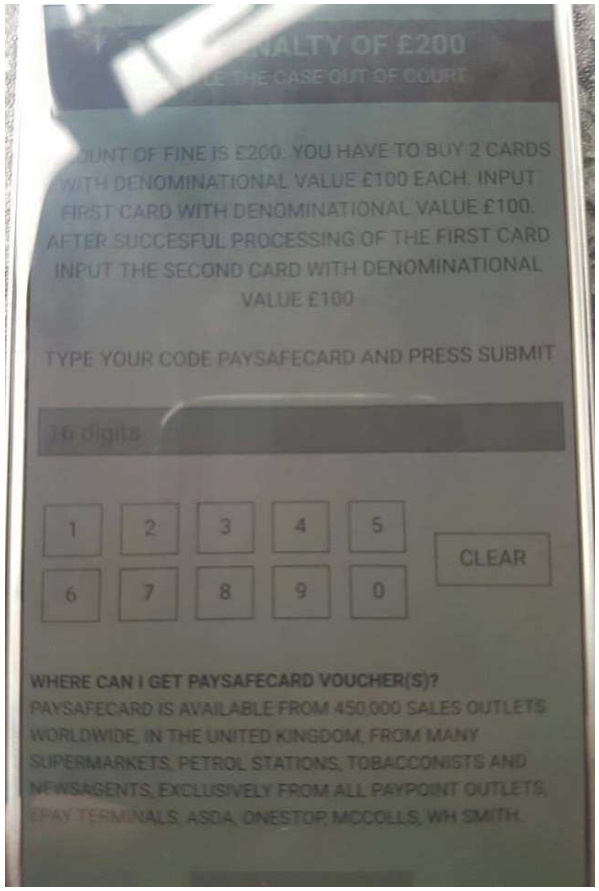
- Trojan, rootkit e backdoor
- Malware infettivi, virus e worm
- Adware
- Ransomware
- Spyware
- Botnet
- Keylogger
- Dialer

Ransomware su PC

Ransomware su smartphone

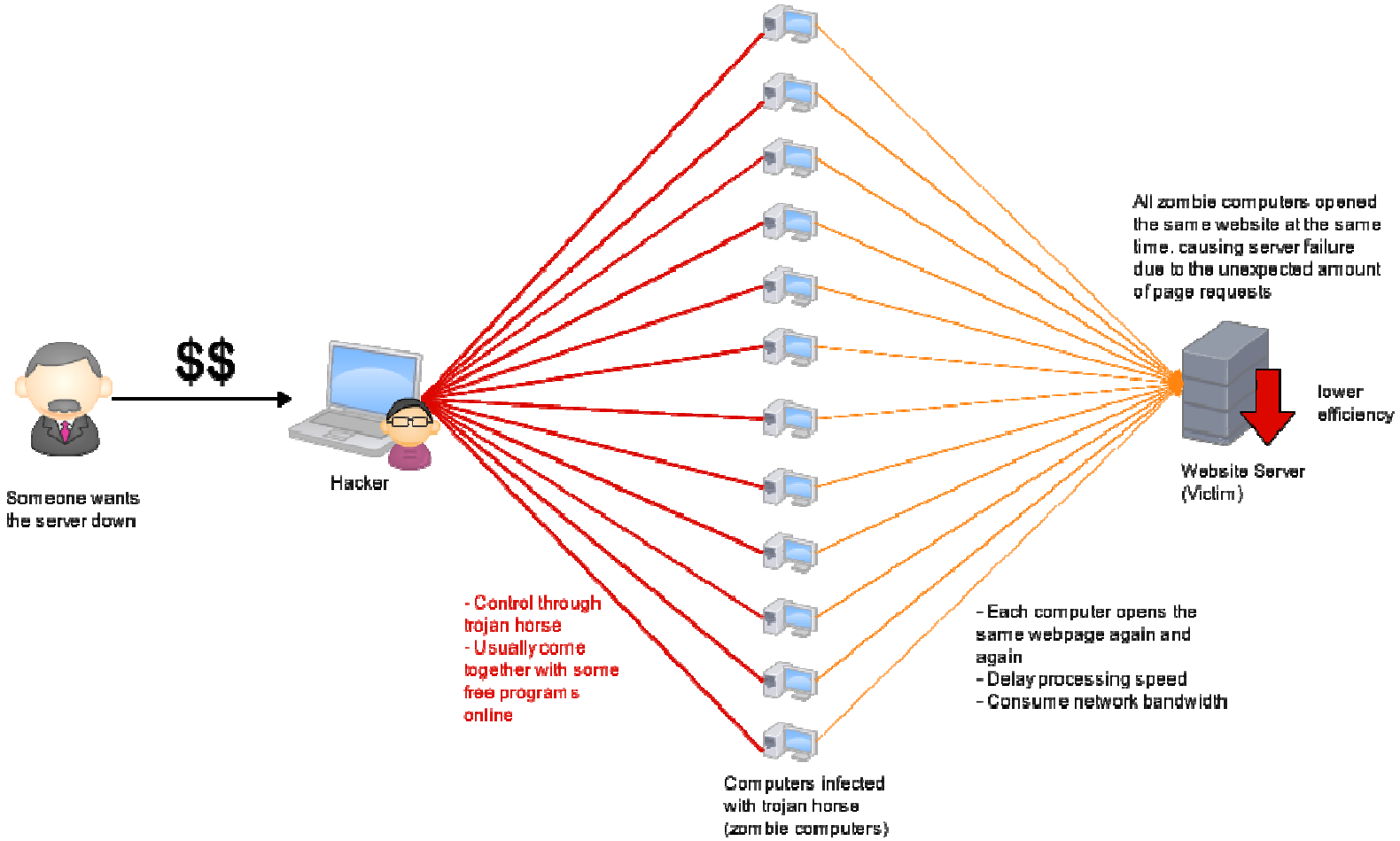






- Diapositive Ransomware CLUSIT

DDOS – Distributed Denial Of Service



2 - Malware

2.2 - Protezione

- Software antivirus: motore di scansione + firme.
- Software antivirus su tutti i sistemi informatici.
- Aggiornare regolarmente vari tipi di software, quali: antivirus, browser web, plug-in, applicazioni, sistema operativo.
- Eseguire scansioni di specifiche unità, cartelle, file usando un software antivirus. Pianificare scansioni usando un software antivirus.
- Rischi associati all'uso di software obsoleto e non supportato, quali: maggiori minacce da parte del malware, incompatibilità.

2 - Malware

ATENEO INTERNAZIONALE
Università per Stranieri di Siena

2.3 – Risoluzione e rimozione

- Quarantena
- Mettere in quarantena, eliminare file infetti/sospetti.
- Un attacco da malware può essere diagnosticato e risolto usando risorse online quali: siti web di sistemi operativi, antivirus, fornitori di browser web, siti web di autorità preposte.

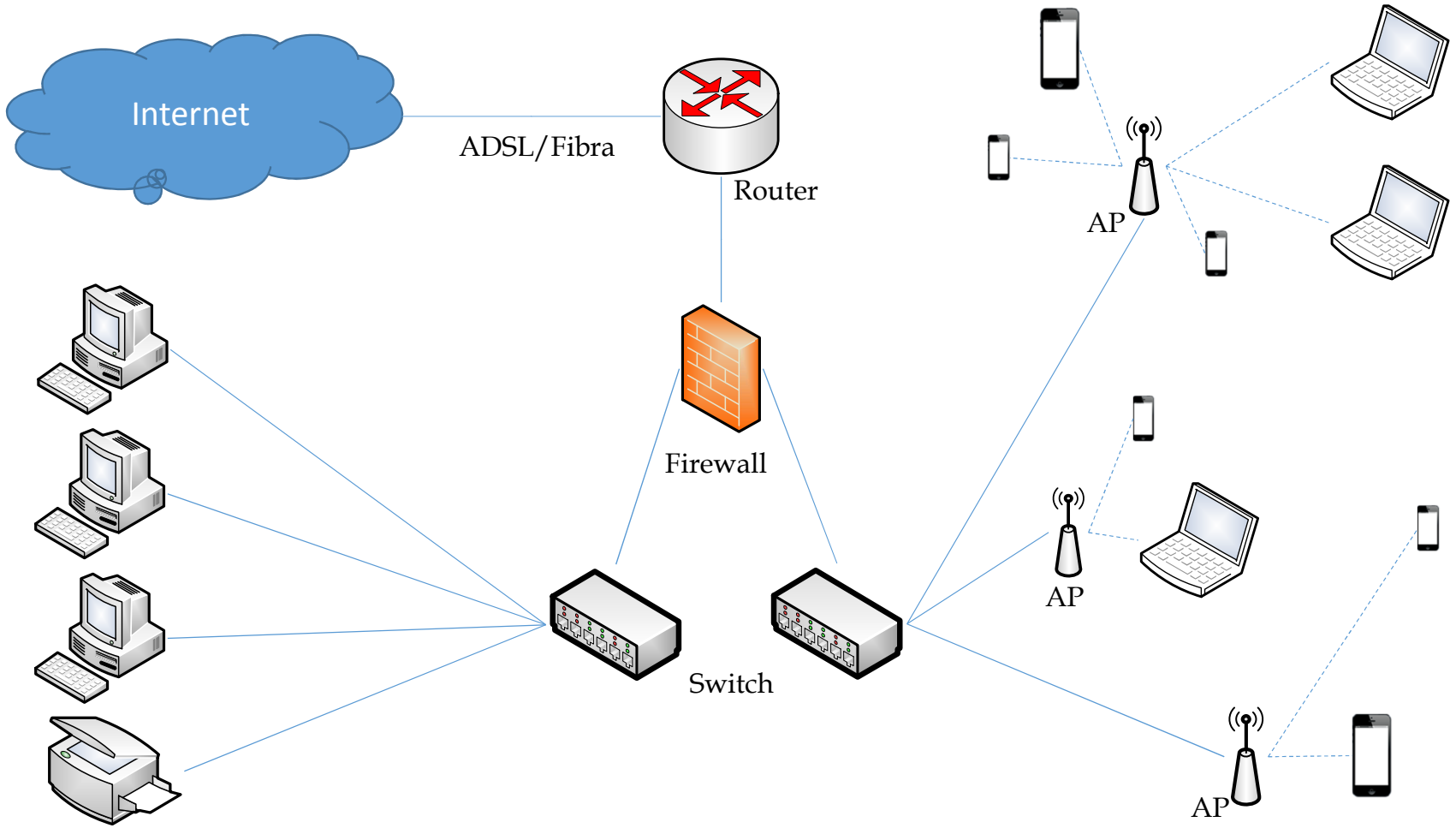
3 - Sicurezza in rete

ATENEO INTERNAZIONALE
Università per Stranieri di Siena

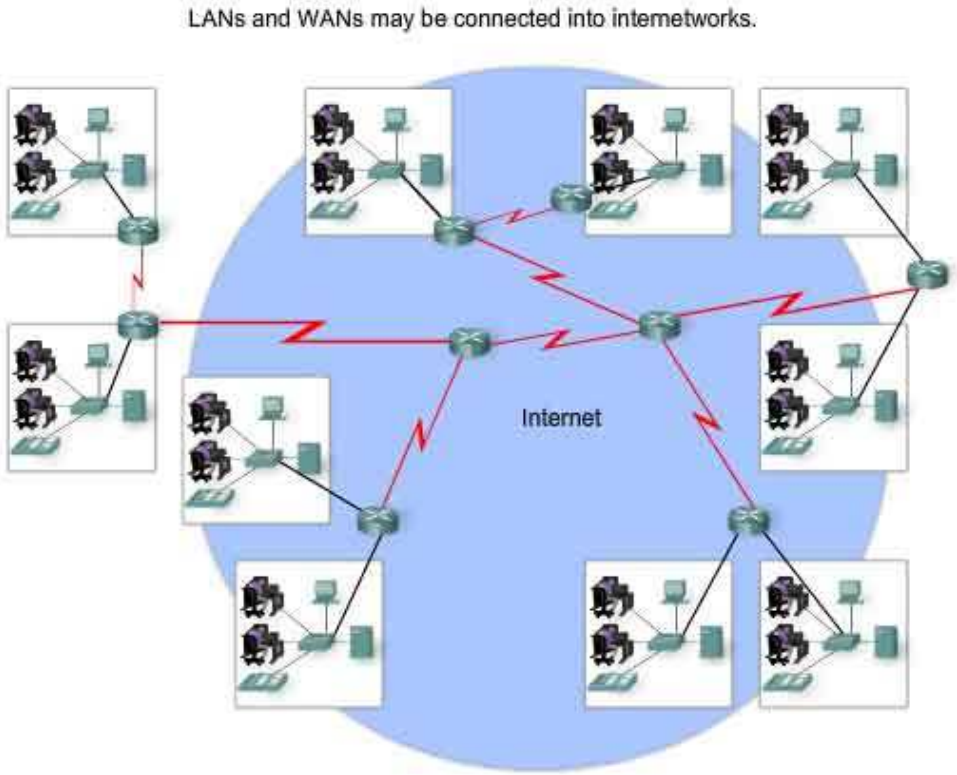
3.1 - Reti e connessioni

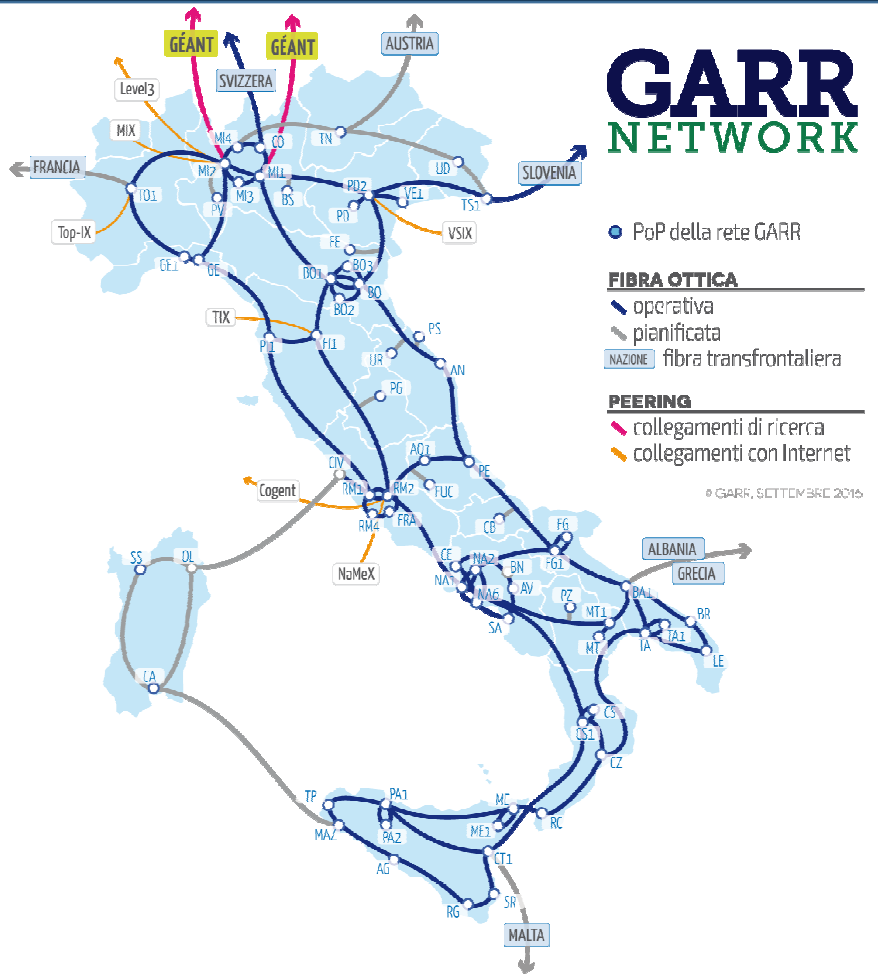
- Reti di computer
  - LAN (rete locale),
  - WLAN (rete locale wireless)
  - WAN (rete geografica)
  - VPN (rete privata virtuale).
- Amministratore di rete:
  - autenticazione, autorizzazione e assegnazione degli account
  - verifica e installazione di patch e aggiornamenti di sicurezza importanti
  - controllo del traffico di rete
  - trattamento del malware rilevato su una rete.
- Firewall in ambiente domestico e di lavoro.

Esempio di rete LAN e WLAN

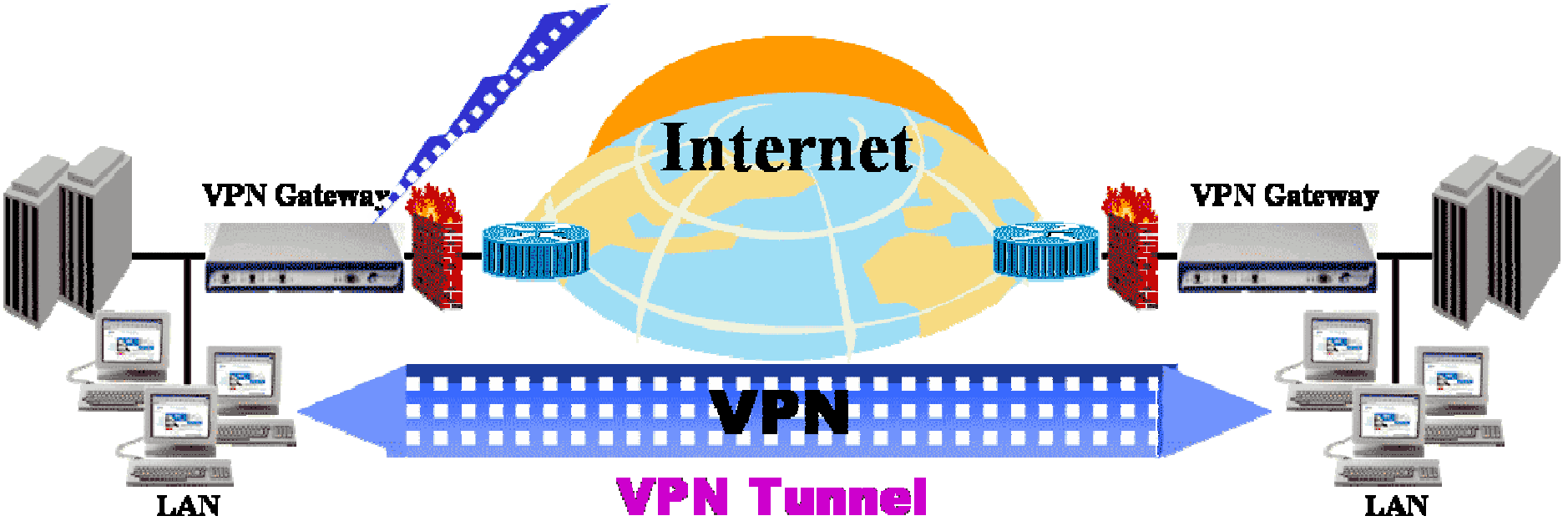


Esempio Reti WAN

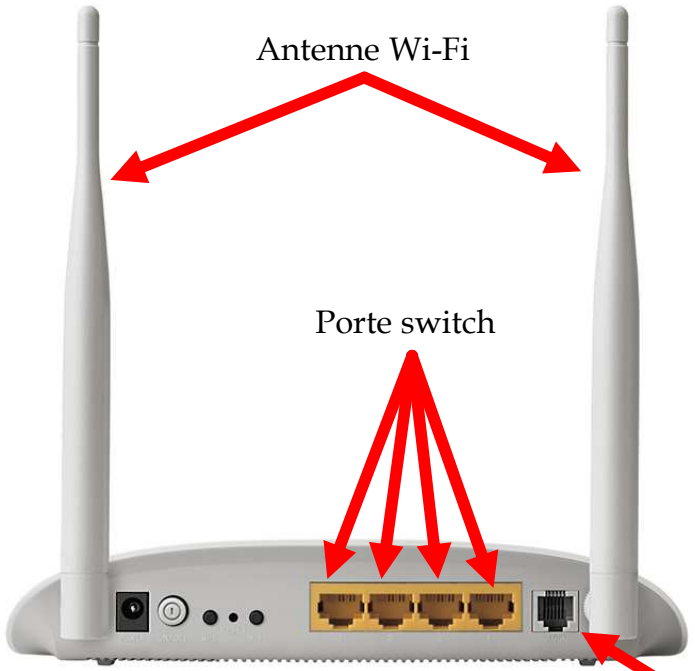




Esempio VPN

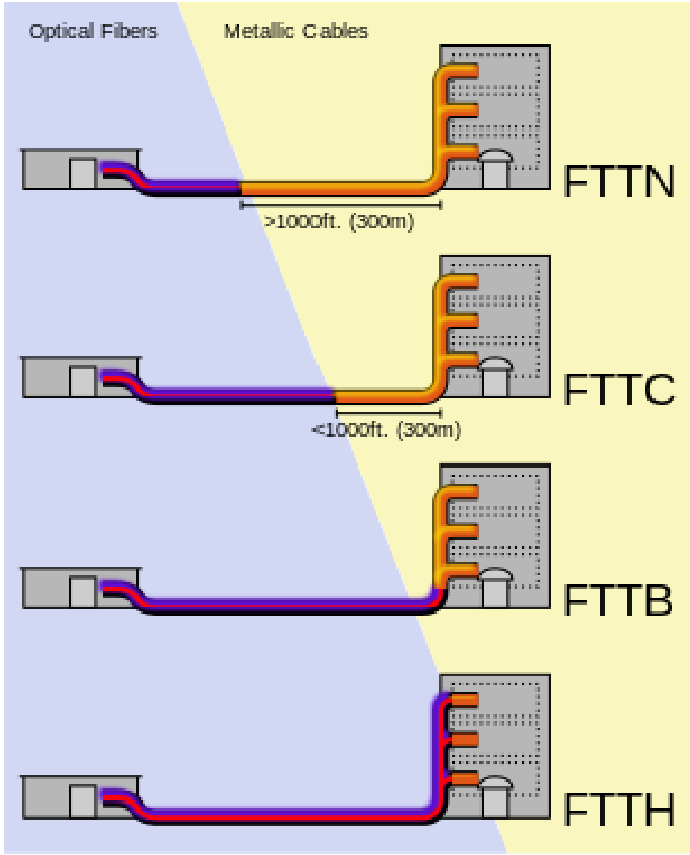


Modem-Router domestico



Connettività internet

Tecnologia	Download	Upload
Dial-up	56kbps	56kbps
ISDN	64/128kbps	64/128kbps
ADSL	da 640k a 20Mbps	da 64kbps a 7Mbps
FTTC	da 30 a 100 Mbps	da 5 a 10 Mbps
FTTH	da 50 a 300Mbps	da 10 a 50Mbps



3 - Sicurezza in rete

3.2 – Sicurezza su reti wireless

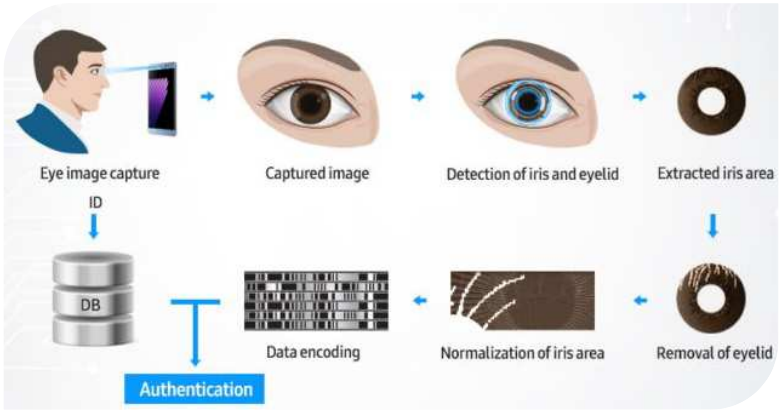
- Tipi di sicurezza per reti wireless
  - WEP (Wired Equivalent Privacy)
  - WPA (Wi-Fi Protected Access) / WPA2 (Wi-Fi Protected Access 2)
  - filtraggio MAC (Media Access Control),
  - SSID nascosto (Service Set Identifier).
- Rete wireless non protetta
  - intercettatori (eavesdropping)
  - dirottatori di rete (network hijacking)
  - violatori di comunicazioni private (man in the middle).
- Hotspot personale

4 – Controllo di accesso

ATENEO INTERNAZIONALE
Università per Stranieri di Siena

4.1 - Metodi

- Impedire accessi non autorizzati ai dati: nome utente, password, PIN, cifratura, autenticazione a più fattori.
- OTP (one-time password)
- Account di rete
- Accedere alla rete con nome utente e password
- Disconnettere l'account al termine
- Tecniche di sicurezza biometrica usate per il controllo degli accessi,impronte digitali, scansione dell'occhio, riconoscimento facciale, geometria della mano.



Minority Report (2002) - Iris scan

4 – Controllo di accesso

5.1 – Gestione delle password

- Buone linee di condotta per la password:
  - scegliere le password di lunghezza adeguata
  - numero sufficiente di lettere, numeri e caratteri speciali
  - evitare parole di sport, compleanni, nomi comuni, hobby, marche e film
  - evitare di condividerle
  - modificarle con regolarità
- Scegliere password diverse per servizi diversi.
- Software di gestione delle password.

WarGames (1983) – The password

WarGames (1983) – Hacking the school

Password più usate (2016)

1. 123456
2. 123456789
3. qwerty
4. 12345678
5. 111111
6. 1234567890
7. 1234567
8. password
9. 123123
10. 987654321
11. qwertyuiop
12. mynoob
13. 123321
14. 666666
15. 18atcskd2w
16. 7777777
17. 1q2w3e4r
18. 654321
19. 555555
20. 3rjs1la7qe
21. google
22. 1q2w3e4r5t
23. 123qwe
24. zxcvbnm
25. 1q2w3e

Ricerca condotta su 10 milioni di password da Keeper Security. Le 25 password più comuni rappresentano il 50% dell'intero campione

Tool di controllo password

http://www.passwordmeter.com/

https://password.kaspersky.com/it/

Balle spaziali (1987)

Riepilogando con un po' di buon umore…

SECURITY TIPS

(PRINT OUT THIS LIST AND KEEP IT IN YOUR BANK SAFE DEPOSIT BOX.)

- DON'T CLICK LINKS TO WEBSITES
- USE PRIME NUMBERS IN YOUR PASSWORD
- CHANGE YOUR PASSWORD MANAGER MONTHLY
- HOLD YOUR BREATH WHILE CROSSING THE BORDER
- INSTALL A SECURE FONT
- USE A 2-FACTOR SMOKE DETECTOR
- CHANGE YOUR MAIDEN NAME REGULARLY
- PUT STRANGE USB DRIVES IN A BAG OF RICE OVERNIGHT
- USE SPECIAL CHARACTERS LIKE & AND %
- ONLY READ CONTENT PUBLISHED THROUGH TOR.COM
- USE A BURNER'S PHONE
- GET AN SSL CERTIFICATE AND STORE IT IN A SAFE PLACE
- IF A BORDER GUARD ASKS TO EXAMINE YOUR LAPTOP, YOU HAVE A LEGAL RIGHT TO CHALLENGE THEM TO A CHESS GAME FOR YOUR SOUL.

Fonte: https://xkcd.com/1820/

5 – Uso sicuro del web

ATENEO INTERNAZIONALE
Università per Stranieri di Siena

5.1 - Impostazioni del browser

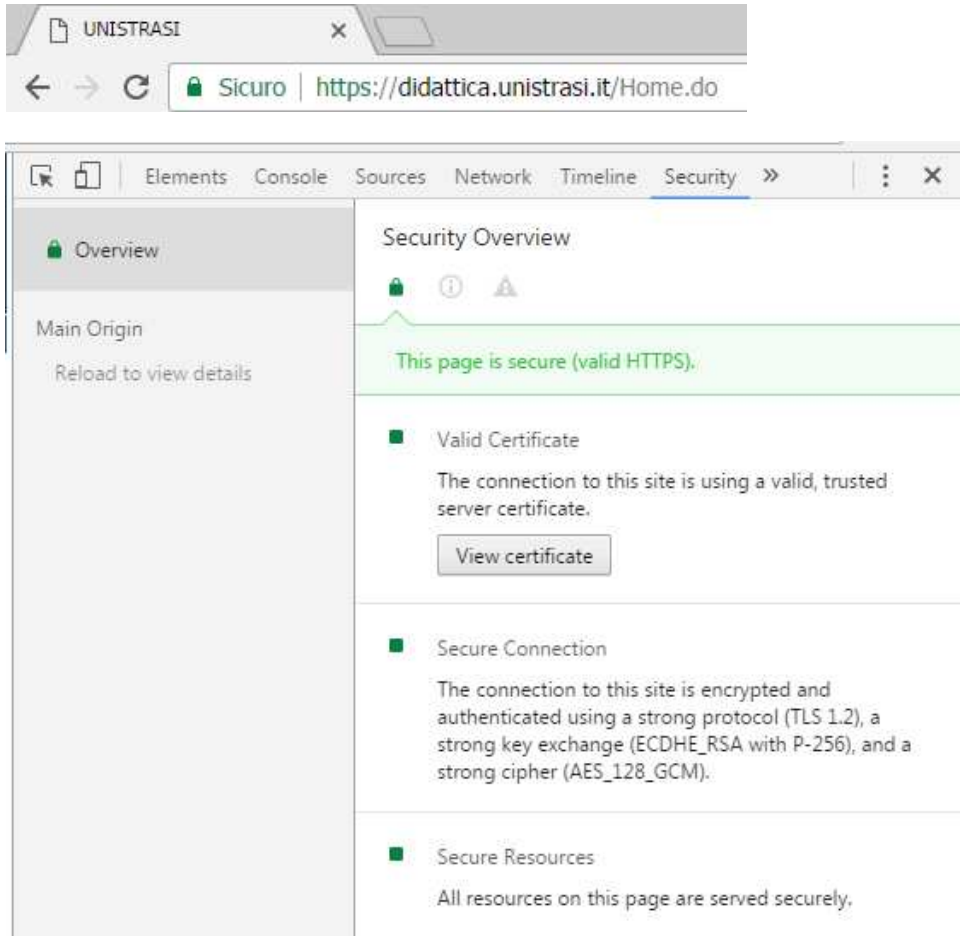
- Selezionare impostazioni adeguate per attivare, disattivare il completamento automatico, il salvataggio automatico quando si compila un modulo.
- Eliminare dati privati da un browser, quali cronologia di navigazione, cronologia di scaricamento, file temporanei di internet, password, cookie, dati per il completamento automatico.

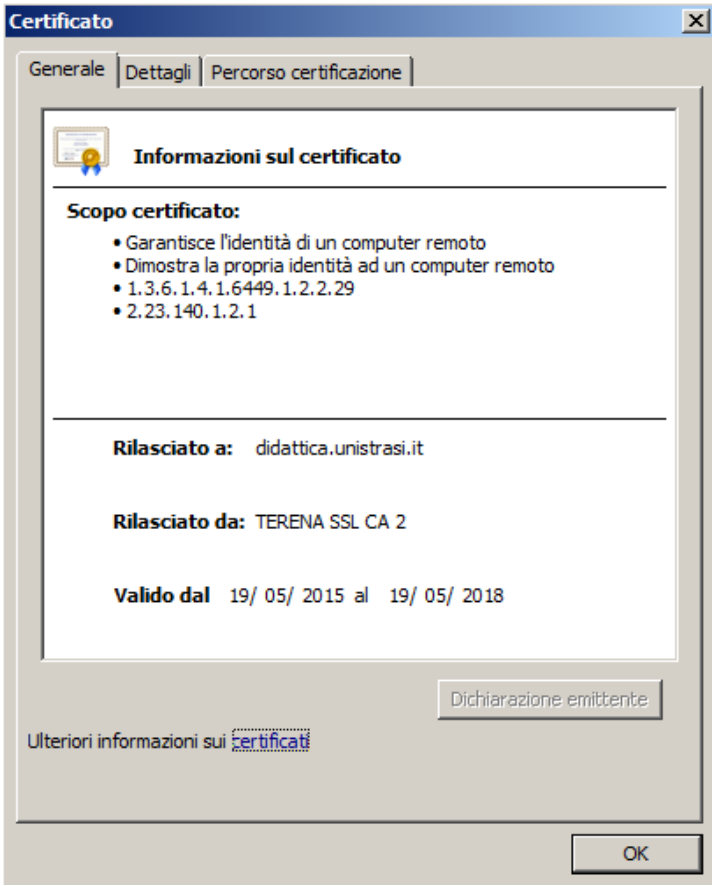
5 – Uso sicuro del web

5.2 – Navigazione sicura in rete

- Acquisti e transazioni finanziarie devono essere eseguite solo su pagine web sicure e con l'uso di una connessione di rete sicura: HTTPS
- Autenticità di un sito web: qualità del contenuto, attualità, validità URL, informazioni sulla società o sul proprietario, informazioni di contatto, certificato di sicurezza, validazione del proprietario del dominio.
- Pharming
- Software per il controllo del contenuto, filtraggio di internet, controllo genitori.

Esempio di sito sicuro – protocollo HTTPS





Pharming - Spoofed URL

- http://mobile.paypal.com.quantisolditirubo.com
- https://mobile.paypal.com

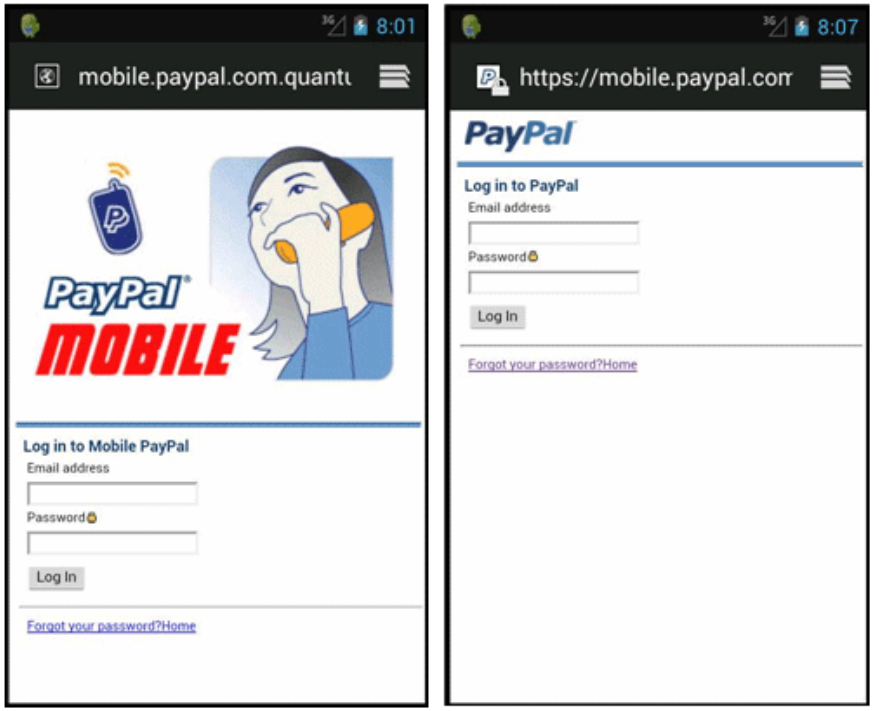


Figure 3. Fake *PayPal* for mobile (left) vs. legitimate site (right)

6 - Comunicazioni

ATENEO INTERNAZIONALE
Università per Stranieri di Siena

6.1 - Posta elettronica

- Cifrare, decifrare un messaggio di posta elettronica.
- Comprendere il termine "firma digitale".
- Identificare i possibili messaggi fraudolenti o indesiderati
- Identificare le più comuni caratteristiche del phishing, quali: uso del nome di aziende e di persone autentiche, collegamenti a falsi siti web, uso di loghi e marchi falsi, incoraggiamento a divulgare informazioni personali.
- Possibilità di denunciare tentativi di phishing alle organizzazioni competenti o alle autorità preposte.
- Rischio di infettare un computer o un dispositivo con malware attraverso l'apertura di un allegato contenente una macro o un file eseguibile.

6.2 – Reti sociali

- Non divulgare su siti di reti sociali informazioni riservate o informazioni personali che permettono l'identificazione.
- Applicare le impostazioni degli account di reti sociali: riservatezza dell'account e propria posizione.
- Pericoli potenziali connessi all'uso di siti di reti sociali, quali cyber bullismo, adescamento (grooming), divulgazione dolosa di informazioni personali, false identità, link o messaggi fraudolenti o malevoli.
- Denunciare usi o comportamenti inappropriati della rete sociale al fornitore del servizio o alle autorità preposte.

Dall'Altra Parte - Spot contro la pedofilia e adescamento online (2012)

6.3 - VoIP e messaggistica istantanea

- Vulnerabilità di sicurezza della messaggistica istantanea e del VoIP (Voice over IP)
  - Malware
  - accesso da backdoor
  - accesso a file
  - intercettazione (eavesdropping).
- Confidenzialità durante l'uso della messaggistica istantanea e del VoIP (Voice over IP)
  - Cifratura
  - non divulgazione di informazioni importanti
  - limitazione alla condivisione di file

WarGames (1983) – Backdoor to Joshua

6.4 – Dispositivi mobili

- Implicazioni dell'uso di applicazioni provenienti da "app store" non ufficiali, quali malware per dispositivi mobili, utilizzo non necessario delle risorse, accesso a dati personali, bassa qualità, costi nascosti.
- Comprendere il termine "autorizzazioni dell'applicazione".
- Applicazioni mobili possono estrarre informazioni private dal dispositivo mobile, quali dettagli dei contatti, cronologia delle posizioni, immagini.
- Misure precauzionali e di emergenza da adottare in caso di perdita di un dispositivo mobile, quali disattivazione remota, cancellazione remota dei contenuti, localizzazione del dispositivo.

7 – Gestione sicura dei dati

7.1 - Messa in sicurezza e salvataggio dei dati

- Sicurezza fisica di computer e dispositivi mobili:
  - non lasciarli incustoditi
  - registrare la collocazione e i dettagli degli apparati
  - usare cavi antifurto
  - controllare gli accessi alle sale dei computer.

7 – Gestione sicura dei dati

ATENEO INTERNAZIONALE
Università per Stranieri di Siena

7.1 - Messa in sicurezza e salvataggio dei dati

7 – Gestione sicura dei dati

ATENEO INTERNAZIONALE
Università per Stranieri di Siena

7.1 - Messa in sicurezza e salvataggio dei dati

- Copie di sicurezza
  - regolarità/frequenza
  - Pianificazione
  - collocazione del supporto dei dati salvati
  - compressione dei dati.
- Supporto di destinazione
  - unità disco/dispositivo locale
  - unità esterna
  - servizio su cloud
- Ripristinare i dati

Esempio di backup policy

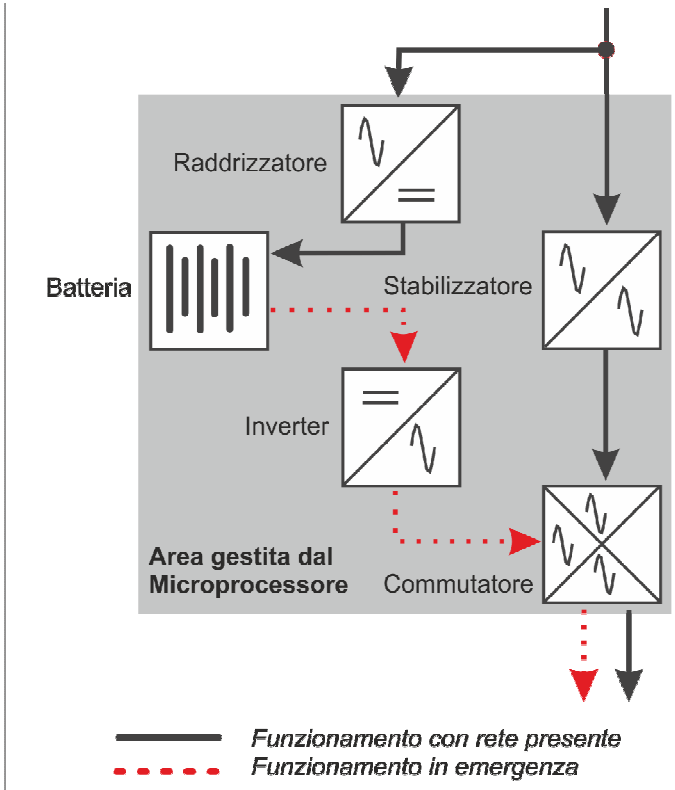
Dimensione	Lunedì	Martedì	Mercoledì	Giovedì	Venerdì	Sabato	Domenica
Esempio	Incrementale	Incrementale	Incrementale	Incrementale	Incrementale	Incrementale	Completo
Settimana 1	*550 Mb*	*700 Mb*	*240 Mb*	*1,8 Gb*	*2,3 Gb*	*600 Mb*	*3,2 Tb*
Settimana 2	*240 Mb*	*3,6 Gb*	*1,2 Gb*	*580 Mb*	*150 Mb*	*180 Mb*	*3,3 Tb*

1 Kb = 1024 byte
1 Mb = 1024 Kb
1 Gb = 1024 Mb
1 Tb = 1024 Gb


BACKUP
Quella cosa che andava fatta prima
@vitadainformatici

UPS – Gruppo di continuità

- Uninterruptable Power Supply



7 – Gestione sicura dei dati

7.2 - *Cancellazione e distruzione sicura*

- Cancellare i dati ≠ eliminarli in modo permanente.
- Eliminazione del contenuto dai servizi online potrebbe non essere permanente (reti sociali, blog, forum su internet, servizi su cloud)
- Distruggere i dati in modo permanente
  - trita documenti
  - distruzione di memorie di massa/dispositivi
  - smagnetizzazione
  - software per la cancellazione definitiva dei dati.

Argo (2012) - L'importanza della distruzione a frammento