



STeP

***Sicurezza informatica: Nozioni di base
Come proteggere il proprio computer
Suggerimenti e linee guida***



■ Virus

- Programmi maliziosi che attaccano una macchina normalmente a seguito di un intervento umano come l'apertura di un allegato di posta, l'inserimento e la lettura di un floppy disk, pen drive, etc.



■ WORM (Verme strisciante)

- Simili ai virus, una volta lanciati, attaccano una macchina sfruttando le **vulnerabilità** note e in caso di successo tentano di duplicarsi automaticamente passando ad attaccare altri sistemi in modo incontrollato



Le minacce della rete

3

- **Trojan horse**
 - Programmi che permettono di installare altri programmi di amministrazione remota “back door” che consentono ad un intruso di infettare il vostro pc con virus e carpire informazioni.
- **Back door**
 - BackOrifice, Netbus e SubSeven sono i programmi più comunemente usati per le intrusioni



■ Spyware

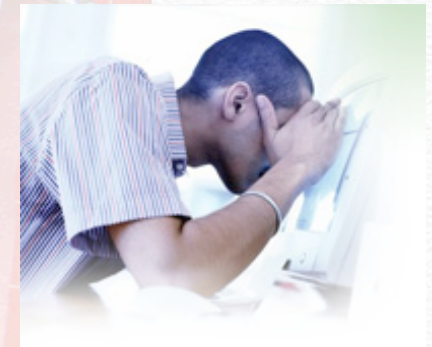
- E' un software che si installa senza consenso dell'utente con lo scopo di raccogliere informazioni riguardo l'utente

- Effetti dello spyware

- Bombardamento di pubblicità
- Raccolta dati personali
- Modifica impostazioni pc
- Rallentamento/arresto del pc

■ Intrusioni

- Accesso ed uso non autorizzato di un sistema



■ Phishing

- Attività criminale che utilizza la tecnica “social engineering”
- “Phishers” tentano di acquisire in modo fraudolento informazioni personali/sensibili
- Furto di identità: password (PIN), numeri di carta di credito etc
- Per attuare le truffe utilizzano e-mail ingannevoli e falsi siti web



■ Attacco a FINECO

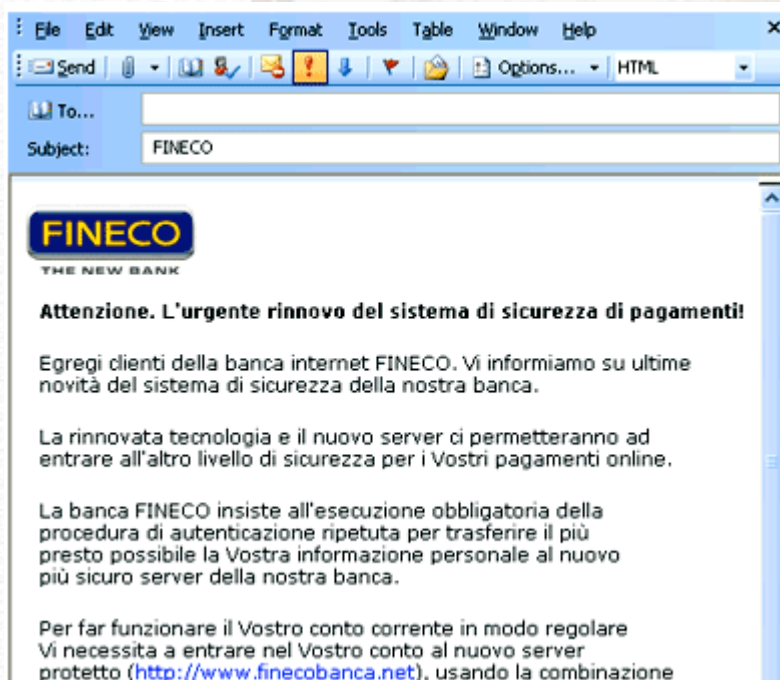
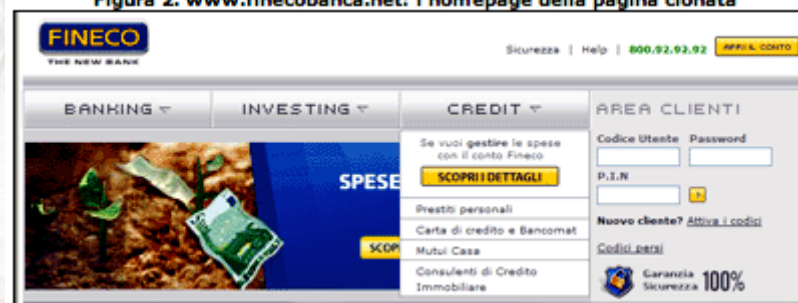


Figura 2. www.finecobanca.net: l'homepage della pagina clonata



Accorgimenti



- **Controllare che l'indirizzo associato al “link” sia corretto**

<https://www.bancawoodgrove.com/loginscript/user2.jsp>

<http://192.168.255.205/wood/index.html>

- **Controllare che il vostro browse abbia aperto una connessione sicura quando inserite una password**

Accedi al conto:

1. Nome utente: 2. Password:

3. Accedi a:

Servizi conto

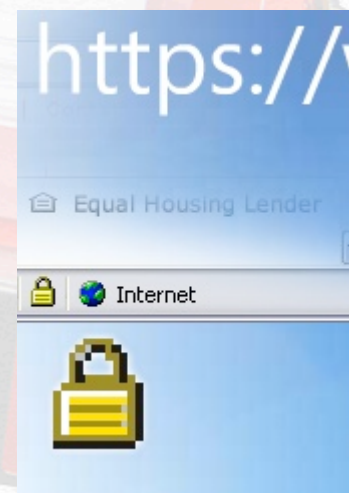
Banking online con pagamento

Conti correnti e conti di de

Panoramica | Conti correnti |

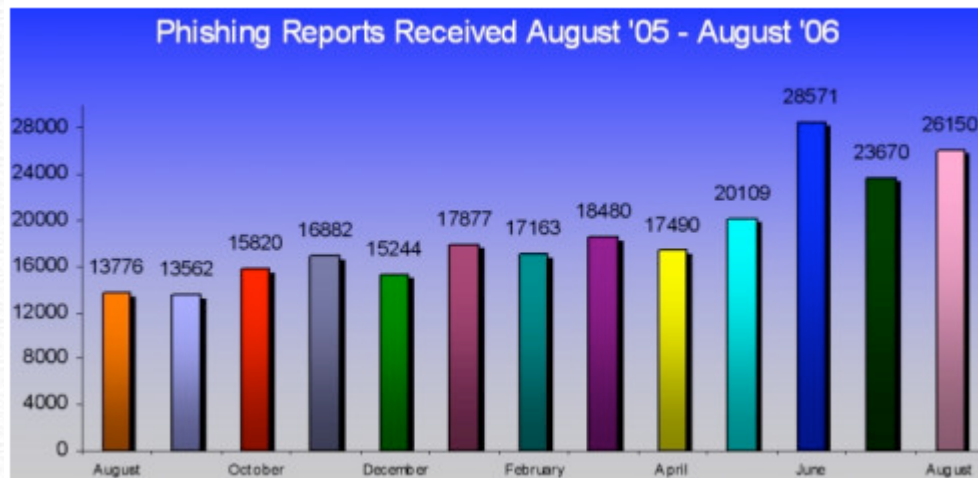
Carte

Carte di credito | Carte di debito



Alcuni dati statistici

■ Phishing



SANS Top-20 Internet Security Attack Targets (2006 Annual Update)



SANS (SysAdmin, Audit, Network, Security) (www.sans.org)

- **Operating Systems**

- W1. Internet Explorer
- W2. Windows Libraries
- W3. Microsoft Office
- W4. Windows Services
- W5. Windows Configuration Weaknesses
- M1. Mac OS XU1.
- UNIX Configuration



SANS Top-20 Internet Security Attack Targets (2006 Annual Update)

10



- **Cross-Platform Applications**
- **C1 Web Applications**
- **C2. Database Software**
- **C3. P2P File Sharing Applications**
- **C4 Instant Messaging**
- **C5. Media Players**
- **C6. DNS Servers**
- **C7. Backup Software**
- **C8. Security, Enterprise, and Directory Management Servers**



SANS Top-20 Internet Security Attack Targets (2006 Annual Update)



- **Network Devices**
- N1. VoIP Servers and Phones
- N2. Network and Other Devices Common Configuration Weaknesses
- **Security Policy and Personnel**
- H1. Excessive User Rights and Unauthorized Devices
- H2. Users (Phishing/Spear Phishing)
- **Special Section**
- Z1. Zero Day Attacks and Prevention Strategies

Le cause di incidente

12

La mancanza di una adeguata cultura della sicurezza



■ 4 Passi fondamentali

1. **Installare e avviare un personal “FIREWALL”**
2. **Utilizzare un software antivirus**
3. **Mantenere il sistema operativo sempre aggiornato**
4. **Utilizzare un software antispyware**

Alcuni accorgimenti

1. **Proteggere l'accesso al pc con password non banali**
2. **Mantenere copie di Cartelle e File importanti**
3. **Crittografare i dati personali/sensibili**
4. **Fare attenzione ai programmi che si installa scaricandoli dalla rete**

Altri accorgimenti

- **Software scaricato via rete**
 - **Non eseguite programmi di cui non siete certi (provenienza/funzionalità)**
- **Allegati di posta elettronica**
 - **Non apriteli - scaricateli e sottoponeteli a scansione virale**
- **Disabilitare Java, Javascript e ActiveX (configurazione browser)**
- **Disabilitare le funzionalità di scripting del client di posta elettronica**

Altri accorgimenti

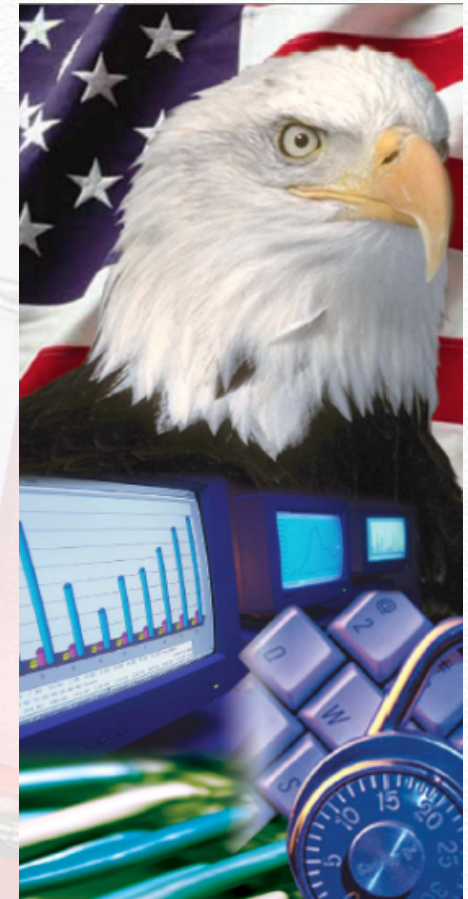
- **NON Codivisione cartelle Windows senza protezione**
- **Abilitare l'entensione dei file (di default disabilitata)**
 - **Downloader (MySis.avi.exe or QuickFlick.mpg.exe)**
- **Disabilitare programmi di “Chat” (IRC) e “instant messaging”**
- **Disabilitare l'attivazione di “link” direttamente dal testo delle e-mail**

Cosa NON fare

- **Non lasciare il proprio pc incustodito (attivare un salva schermo con password)**
- **Non lasciare la password scritta su un "post-it" attaccato allo schermo**
- **Non installare programmi di tipo "Peer TO Peer" per scaricare musica e/o altro sui sistemi che mantengono dati personali**

Password

- **Utilizzare password complesse**
 - **Usare una combinazione di numeri, simboli e lettere (maiuscole e minuscole)**
- **Cambiare la password ogni 45/90 giorni**
- **Non dare a nessuno il proprio username, password, o altro codice di accesso a computer o servizi**



Incidenti Informatici

- **Definiamo incidente informatico qualunque azione o concomitanza di eventi accidentali e/o volontari che porti alla violazione dei requisiti di:**
 - **Disponibilita'**
 - Interruzione non autorizzata totale o parziale di servizi (DOS)
 - **Integrita'**
 - Perdita di informazioni o modifica non autorizzata di dati
 - **Riservatezza**
 - Accesso a sistemi (Intrusione) o intercettazione di dati non autorizzato
 - **Uso improprio e non autorizzato di risorse informatiche**
 - Falsificazione di identita' o di documenti
 - Invio non autorizzato di e-mail (SPAM) (*)

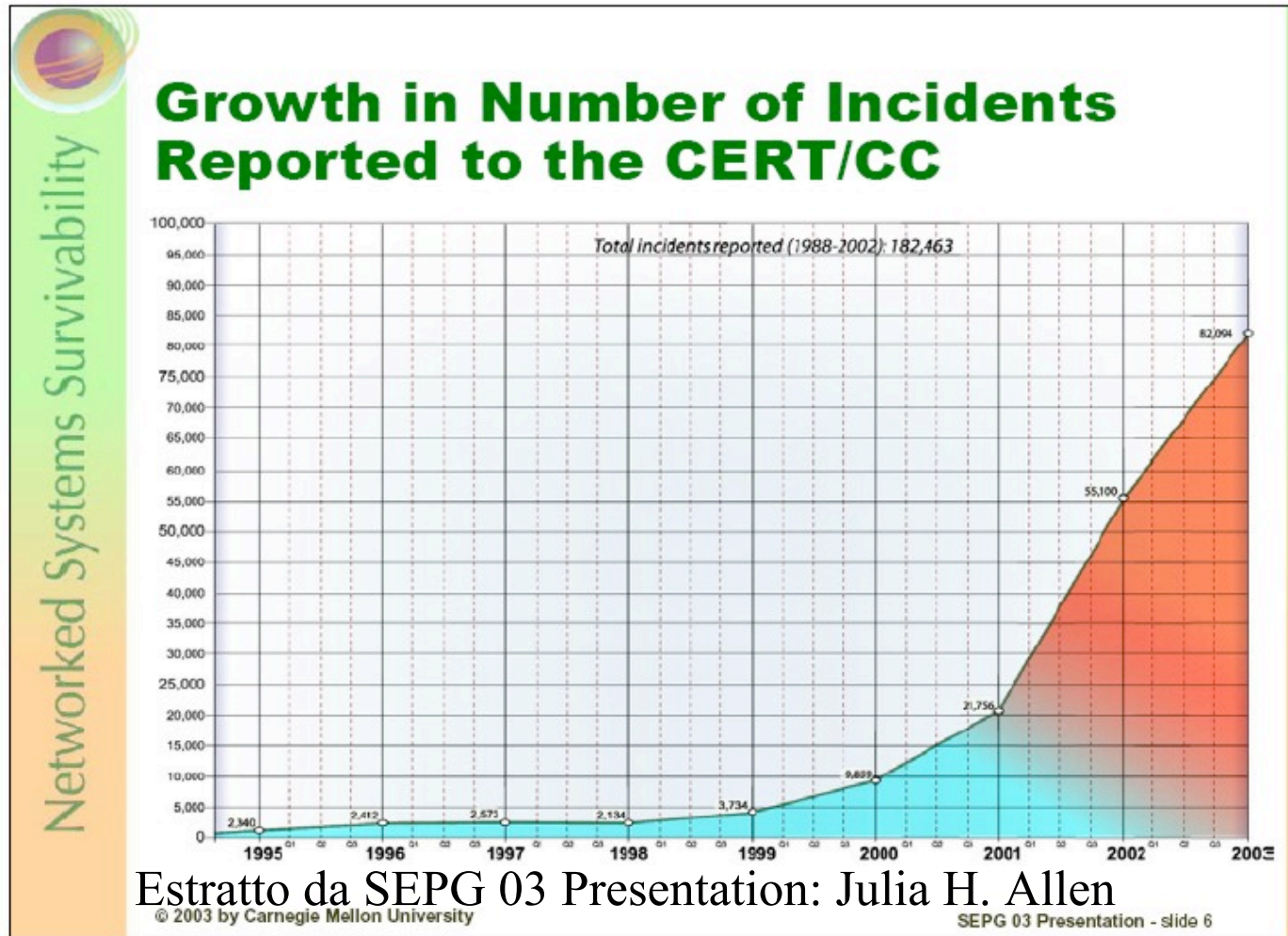
Andamento incidenti

Incidenti segnalati



Incidenti non segnalati

Andamento Incidenti



Facciamo due conti

- **Costo orario di un dipendente Eu. 90**
- **Un virus provoca un fermo di circa 4 ore (blocco macchina, ricerca istruzioni/tool di rimozione, ripristino aggiornamento antivirus/sistema etc)**
- **SPAM richiedono 2/3 minuti al giorno procapite**

Ovvero ...

- **Supponendo:**

- **2 virus anno = 8 ore lav = 720,00 E**

- **SPAM 2m x 240gg = 480,00 E**

spesa pro-capite = 1.200,00 E

100 dipendenti = 120.000,00E

Alcuni riferimenti

- **Microsoft (guide e software)**
 - www.microsoft.com/italy/athome/security/

- **Antivirus**
 - www.grisoft.com
 - www.trendmicro.com
 - www.virus.org

- **Firewall/Antispyware**
 - www.zonelabs.com
 - www.lavasoft.com
 - www.safer-networking.org



Grazie dell'attenzione