

## Indice

1. CYBERCRIME
2. NOTIZIE E SEGNALAZIONI DAI SOCI
3. MAGGIORE ESPERIENZA PER CERTIFICARSI CISSP
4. EVENTI SICUREZZA

### 1. CYBERCRIME

#### **Phishing.**

In quest'ultimo periodo vi è stato un incremento nel numero e tipologia di email di phishing. Le Aziende attaccate sono prevalentemente:

Banca di Roma / Capitalia; eBay; Banca Intesa; Banca Sella; Banco di Sicilia; Poste Italiane.

Abbiamo individuato almeno 5 varianti di "esche".

Adducendo ogni volta una differente scusa (l'esca, appunto), i criminali cercano di far abboccare un ipotetico incosciente (o ignorante) correntista ad accedere al sito indicato nella email e lì fargli inserire i suoi codici segreti (e da quel momento non lo sono più!).

#### **Le esche più frequenti:**

- è richiesta la verifica dei dati del correntista per motivi di sicurezza;
- il conto è stato bloccato (segue la motivazione del blocco, quale ad esempio aver digitato troppe volte un codice errato, e quindi le indicazioni per ripristinarlo);
- accedere ad un conto più sicuro (.e.. vai! più sicuro di così!);
- si ha diritto ad un premio (sic!);
- è stata portata a termine una presunta richiesta di pagamento a terzi e quindi il conto corrente è stato addebitato dell'importo indicato (segue collasso dello sprovveduto correntista per un ingiustificato addebito e, a questo punto, il suo "abboccare" all'amo inserendo i dati personali!).

Sul sito abbiamo riportato alcuni di questi esempi.

I sistemi di antispam in commercio, in genere, si accorgono che qualcosa non va in questi messaggi e li segnala come SPAM, ma ciò non avviene sempre, data anche la difficoltà di interpretazione ed il rischio di errori, con conseguente lamentela da parte del Cliente.

Le banche, oltre a migliorare i sistemi di sicurezza, monitorizzano la rete e grazie all'intervento delle Autorità (in particolare della Polizia delle Comunicazioni e del GAT), vengono bloccati i siti criminali.

Trattasi però di una lotta senza fine: ad ogni "bastione" di difesa creato corrisponde un attacco nuovo !!!!

Non ultimo, i cyber criminali stanno mettendo in cantiere altre tecniche, più sofisticate (nel documento sopra citato abbiamo anche riportato un invito a leggere una presunta cartolina di auguri: questa tipologia di email tende a far scaricare sul computer del Cliente un software

malevolo che successivamente agisce in modo assai pericoloso e subdolo).

**Il Consumatore, il Correntista, il Cliente, deve capire due regole fondamentali:**

- non dare mai le proprie credenziali (codice utente, password, numero del conto, ecc.) o dati strettamente personali a qualcuno che ce le chiede, per nessun motivo, qualsiasi sia il canale adottato (email, telefono, citofono, alla porta, ecc.); si deve sempre verificare la veridicità della richiesta telefonando o andando in banca, parlandone con un responsabile se del caso;
- il computer va dotato dei necessari software che ne garantiscano il funzionamento e la protezione, e li aggiorni frequentemente (quanti non hanno software di protezione perché accedono a siti. o non vogliono spendere 50 euro per un software?).

Alla luce di queste e di altre considerazioni che qui, per brevità non stiamo a descrivere, abbiamo predisposto - a distanza di due anni dal precedente - un nuovo volumetto in accordo con ADICONSUM da distribuire ai Consumatori, onde sensibilizzarli ricordando loro poche ma semplici regole.

Il volumetto verrà distribuito in Italia quest'autunno.

Nel frattempo abbiamo ritenuto opportuno monitorare i sistemi di difesa degli intermediari finanziari, in quanto non ci sembra che tutte le Aziende utilizzino appieno le tecnologie che il mercato offre: ciò crea una disparità che finisce con il confondere il Consumatore che, a fronte di messaggi rassicuranti della propria banca, legge sui giornali testimonianze di perdite economiche su Internet anche considerevoli.

Fonte: ANSSAIF [www.anssaif.it](http://www.anssaif.it)

---

Ancora un caso di arresto per accesso non autorizzato a reti wireless.

Si tratta di un cittadino britannico, sorpreso dalla polizia mentre navigava in rete utilizzando la connessione di un altro.

Fonte: <http://news.bbc.co.uk/1/hi/england/london/6958429.stm>

Interessanti le considerazioni apparse al proposito su [www.zone-h.it/content/view/676/9](http://www.zone-h.it/content/view/676/9)

## **2. NOTIZIE E SEGNALAZIONI DAI SOCI**

***La deadline per l'invio di eventuali segnalazioni dei soci per la pubblicazione sulla newsletter è il 25 di ogni mese***

---

Il prossimo 10 Settembre si terrà a Roma il convegno dal titolo: "Privacy in the 21th Century", organizzato da OWASP-Italy in collaborazione con il Master in Sicurezza Informatica dell'Università La Sapienza.

Tale convegno si tiene nell'ambito dell' OWASP Day, che è il giorno in cui sono organizzati convegni multipli dai vari local OWASP Chapter nel mondo durante il Global Security Week.

cfr. <http://www.owasp.org>

L'argomento trattato sarà la Privacy nel 21° secolo per quanto concerne la sicurezza delle applicazioni web.

L'evento mostrerà 6 interventi di discussione, nella prima parte si affronterà l'argomento da un punto di vista di alto livello, nella seconda parte sarà lasciato spazio agli interventi più tecnici.

L'obiettivo della conferenza è creare un dibattito su quale è il corrente stato della privacy per la Web Application Security e chi dovrebbe porre attenzione su questo.

Da un punto di vista tecnico si vuole discutere sulle 3 maggiori fonti di vulnerabilità delle web application e i loro impatti sulla Privacy:

1. CROSS-SITE SCRIPTING
2. SQL INJECTION
3. SESSION EXPOSURE

La manifestazione si terrà presso la sala alfa del Dipartimento di Informatica dell'Università di Roma "La Sapienza", in Via Salaria 113.

L'ingresso è gratuito ma è richiesto l'invio di una mail a [mastersicurezza@di.uniroma1.it](mailto:mastersicurezza@di.uniroma1.it) con oggetto "OWASP Day: Privacy in the 21th Century"

---

## ROMA CAPUT MEDIA! L'AUTUNNO ICT CHE PROIETTA LA CAPITALE NEL MONDO

26-27 Settembre 2007, Marriott Park Hotel – Roma

VON Europe 2007, Broadband Business Forum 2007, Video on the Net Europe 2007, Videogov e Netcomm Roma E-commerce Forum: questi gli eventi internazionali e nazionali che si terranno in co-location a Roma il 26-27 Settembre 2007.

Nel corso della due giorni capitolina i leader del mondo ICT e multimediale presenteranno tutte le ultime novità:

- VMNO, Security & Privacy, Open Source e Mobile VoIP
- Municipal Wireless, WiMax, Reti Mesh
- Web e IP TV, DRM, Video Sharing e Web 2.0
- Videosorveglianza in ambito pubblico, in particolare Urban e Homeland Security
- Stato dell'arte sull'eCommerce italiano

Clusit è tra i patrocinatori di VON Europe 2007 e Broadband Business Forum 2007 e contribuirà alla realizzazione di un workshop sulla sicurezza legata all'adozione delle comunicazioni IP based in azienda e agli apparati Wireless e mobili.

Chairman della conferenza sarà Raoul Chiesa, Membro del Comitato Direttivo e del Comitato Tecnico Scientifico del CLUSIT.

Per consultare il Programma della manifestazione, per la registrazione gratuita e per partecipare alle conferenze:

[www.romacaputmedia.com](http://www.romacaputmedia.com)

### 3. MAGGIORE ESPERIENZA PER CERTIFICARSI CISSP

Dal 1° ottobre 2007 entreranno in vigore nuovi termini relativi all'esperienza lavorativa ed all'endorsement.

#### **Esperienza professionale:**

L'esperienza lavorativa richiesta per ottenere la certificazione CISSP® passerà da 4 a 5 anni e deve coprire almeno 2 dei 10 domini del CBK®.

E' rilevante che dei 5 anni di esperienza un anno può essere sostituito da una laurea (almeno quadriennale) ed un secondo anno può essere sostituito da una certificazione di quelle elencate alla pagina <https://www.isc2.org/cgi-bin/content.cgi?page=1016>.

#### **Endorsement:**

Chi avrà passato l'esame per certificarsi CISSP, CAP®, o SSCP® dovrà produrre l'endorsement sottoscritto da persona che abbia già ottenuto una certificazione (ISC)².

Maggiori e più particolareggiate informazioni sono disponibili alla pagina <https://www.isc2.org/cgi-bin/content.cgi?page=1227>.

**Il calendario dei seminari** ed esami CISSP in Italia vede il prossimo appuntamento a Roma:

Dal 22 al 26 ottobre il *seminario*; il 24 novembre *l'esame*.

Per chi passerà l'esame in questa sessione varranno i nuovi termini.

Le modalità di registrazione sono alla pagina [www.clusit.it/isc2/calendario\\_isc2.htm](http://www.clusit.it/isc2/calendario_isc2.htm).

Ogni altra informazione può essere richiesta a [isc2@clusit.it](mailto:isc2@clusit.it)

### 4. EVENTI SICUREZZA

18 settembre 2007, Milano - Seminario Clusit

VoIP (in)security

[https://edu.clusit.it/scheda\\_seminario.php?id=11](https://edu.clusit.it/scheda_seminario.php?id=11)

25 settembre 2007, Milano

La sicurezza dallo A allo z. Le nuove soluzioni per IBM System z

<http://www-306.ibm.com/software/it/events/zsecurity>

25-27 settembre 2007, Roma

The 8th International Common Criteria Conference

[www.8iccc.com/index.php?option=com\\_content&task=view&id=35&Itemid=43](http://www.8iccc.com/index.php?option=com_content&task=view&id=35&Itemid=43)

26-27 settembre 2007, Roma

ROMA CAPUT MEDIA

[www.romacaputmedia.com](http://www.romacaputmedia.com)

---

2 ottobre 2007, Roma - Seminario Clusit

La sicurezza fisica: parte indispensabile della sicurezza delle informazioni  
[https://edu.clusit.it/scheda\\_seminario.php?id=16](https://edu.clusit.it/scheda_seminario.php?id=16)

---

3 ottobre 2007, Roma

La sicurezza dallo A allo z. Le nuove soluzioni per IBM System z  
<http://www-306.ibm.com/software/it/events/zsecurity>

---

9 ottobre 2007, Firenze - Seminario Clusit

VoIP (in)security  
[https://edu.clusit.it/scheda\\_seminario.php?id=13](https://edu.clusit.it/scheda_seminario.php?id=13)

---

16 ottobre 2007, Milano - Seminario Clusit

La sicurezza fisica: parte indispensabile della sicurezza delle informazioni  
[https://edu.clusit.it/scheda\\_seminario.php?id=17](https://edu.clusit.it/scheda_seminario.php?id=17)

---

22-26 ottobre 2007, Roma

Seminario CISSP  
[www.clusit.it/isc2/calendario\\_isc2.htm](http://www.clusit.it/isc2/calendario_isc2.htm)

---

**CLUSIT - ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA\***

Dipartimento di Informatica e Comunicazione  
Università degli Studi di Milano  
Via Comelico 39 - 20135 MILANO - cell. 347.2319285

\* associazione senza fini di lucro, costituita il 4 luglio 2000

**© 2007 Clusit - Vietata la riproduzione**

Clausola di esclusione della responsabilità e informazioni relative al  
Copyright: [www.clusit.it/disclaimer.htm](http://www.clusit.it/disclaimer.htm)