IT-Security

Syllabus 2.0

con NOTE

A Cura di Enzo Exposyto

INDICE

1 CONCETTI di SICUREZZA

1.1 MINACCE ai DATI

1.1.1 Distinguere tra

- **DATI**

  e

- **INFORMAZIONI.**

(nota: per DATI e INFORMAZIONI, VEDI MINACCE ai DATI - PARTE 1_1A di Enzo Exposyto, *PAGINE da 12 a 32*.)

1.1.2 Comprendere i termini

- **"CRIMINE INFORMATICO"**

  e

- **"HACKING".**

(nota 1: Per CRIMINE INFORMATICO si intende qualsiasi ATTIVITÀ CRIMINALE svolta utilizzando COMPUTER, DISPOSITIVI INFORMATICI e/o INTERNET.)

(nota 2: per un ELENCO dei CRIMINI INFORMATICI e delle RELATIVE PENE, VEDI MINACCE ai DATI - PARTE 1_1A di Enzo Exposyto, *PAGINE da 33 a 55*.)

(nota 3: l'HACKING è l'INSIEME dei METODI, delle TECNICHE e delle OPERAZIONI per CONOSCERE, ACCEDERE A, MODIFICARE un SISTEMA INFORMATICO, HARDWARE o SOFTWARE.
Per FINI *ILLECITI* o *LECITI*, L'HACKER SI OCCUPA di SICUREZZA INFORMATICA.
Oppure, HACKING: la MANIPOLAZIONE del COMPORTAMENTO NORMALE di COMPUTER e/o ALTRI DISPOSITIVI INFORMATICI e dei RELATIVI SISTEMI ad ESSI CONNESSI.
NON CONFONDERE l'HACKING con il CRACKING: il CRACKER HA COME *UNICO* OBIETTIVO QUELLO di DANNEGGIARE, TRUFFARE e/o DERUBARE PERSONE ed ENTI PRIVATI o PUBBLICI.)

(nota 4: per HACKING e CRACKING, VEDI MINACCE ai DATI - PARTE 1_1A di Enzo Exposyto, *PAGINE da 56 a 58*.)

Vedi pagina successiva

Torna all'INDICE

1 CONCETTI di SICUREZZA

1.1 MINACCE ai DATI

1.1.3 Riconoscere le MINACCE DOLOSE e ACCIDENTALI ai DATI PROVOCATE da

- **SINGOLI INDIVIDUI,**
- **FORNITORI DI SERVIZI,**
- **ORGANIZZAZIONI ESTERNE.**

(nota: per le MINACCE DOLOSE e ACCIDENTALI ai DATI, VEDI MINACCE ai DATI - PARTE 1_1A di Enzo Exposyto, *PAGINE da 59 a 61*.)

1.1.4 Riconoscere le MINACCE ai DATI PROVOCATE da CIRCOSTANZE STRAORDINARIE, quali

- **FUOCO,**
- **INONDAZIONI,**
- **GUERRE,**
- **TERREMOTI.**

(nota: per le MINACCE da CIRCOSTANZE STRAORDINARIE, VEDI MINACCE ai DATI - PARTE 1_1A di Enzo Exposyto, *PAGINE da 62 a 64*.)

1.1.5 Riconoscere le MINACCE ai DATI PROVOCATE dall'USO del CLOUD COMPUTING, quali:

- **CONTROLLO sui DATI,**
- **POTENZIALE PERDITA di RISERVATEZZA (PRIVACY).**

(nota 1: CLOUD COMPUTING, INSIEME dei SERVIZI OFFERTI TRAMITE INTERNET -*quali* l'ARCHIVIAZIONE, l'ELABORAZIONE con APPLICAZIONI ONLINE, la TRASMISSIONE, et cetera di DATI/INFORMAZIONI- da una SOCIETÀ d'INFORMATICA (CLOUD PROVIDER) ai PROPRI CLIENTI.)

(nota 2: per i *TANTI* TIPI di CLOUD COMPUTING e RELATIVE MINACCE ai DATI, VEDI MINACCE ai DATI - PARTE 1_1B di Enzo Exposyto, *PAGINE da 12 a 68*.)

Torna all'INDICE

1 CONCETTI di SICUREZZA

1.2 VALORE delle INFORMAZIONI

1.2.1 Comprendere le CARATTERISTICHE FONDAMENTALI della SICUREZZA delle INFORMAZIONI, quali:

- **CONFIDENZIALITÀ**
- **INTEGRITÀ,**
- **DISPONIBILITÀ.**

(nota 1: CONFIDENZIALITÀ o, anche, RISERVATEZZA; ESSA GARANTISCE la PROTEZIONE dei DATI *CONTRO gli ACCESSI NON AUTORIZZATI*.)

(nota 2: INTEGRITÀ; ESSA GARANTISCE CHE i DATI *NON POSSONO ESSERE MODIFICATI SENZA AUTORIZZAZIONE*.)

(nota 3: per CONFIDENZIALITÀ (RISERVATEZZA), INTEGRITÀ e DISPONIBILITÀ, VEDI VALORE delle INFORMAZIONI - PARTE 1_2A di Enzo Exposyto, *PAGINE da 12 a 39*.)

1.2.2 Comprendere i MOTIVI per PROTEGGERE le INFORMAZIONI *PERSONALI*, quali

- **EVITARE il FURTO di IDENTITÀ**
  o
- **le FRODI,**
- **MANTENERE la RISERVATEZZA.**

(nota: per comprendere i MOTIVI per PROTEGGERE le INFORMAZIONI *PERSONALI*, VEDI VALORE delle INFORMAZIONI - PARTE 1_2B di Enzo Exposyto, *PAGINE da 12 a 16*.)

Vedi pagina successiva

Torna all'INDICE

1 CONCETTI di SICUREZZA

1.2. VALORE delle INFORMAZIONI

1.2.3 Comprendere i MOTIVI per PROTEGGERE INFORMAZIONI *di LAVORO* su computer e dispositivi mobili, quali:

- **EVITARE FURTI,**
- **UTILIZZI FRAUDOLENTI,**
- **PERDITE ACCIDENTALI di DATI,**
- **SABOTAGGI.**

(nota: per comprendere i MOTIVI per PROTEGGERE le INFORMAZIONI *di LAVORO*, VEDI VALORE delle INFORMAZIONI - PARTE 1_2B di Enzo Exposyto, *PAGINE da 17 a 20*.)

1.2.4 Identificare i PRINCIPI COMUNI per la PROTEZIONE, CONSERVAZIONE e CONTROLLO dei DATI e della RISERVATEZZA, quali:

- **TRASPARENZA,**
- **SCOPI LEGITTIMI,**
- **PROPORZIONALITÀ delle MISURE in RAPPORTO ai DANNI.**

(nota: per identificare i PRINCIPI COMUNI …, VEDI VALORE delle INFORMAZIONI - PARTE 1_2B di Enzo Exposyto, *PAGINE da 21 a 25*.)

Vedi pagina successiva

Torna all'INDICE

1 CONCETTI di SICUREZZA

1.2. VALORE delle INFORMAZIONI

1.2.5 Comprendere i TERMINI

- **“SOGGETTI dei DATI”**
  e
- **“CONTROLLORI dei DATI”,**

e come si applicano nei due casi i PRINCIPI di

- **PROTEZIONE,**
- **CONSERVAZIONE**
  e
- **CONTROLLO dei DATI**
  e
- **della RISERVATEZZA.**

(nota: per comprendere i TERMINI …, VEDI VALORE delle INFORMAZIONI - PARTE 1_2B di Enzo Exposyto, *PAGINE da 26 a 41*.)

1.2.6 Comprendere l’IMPORTANZA di ATTENERSI alle

- **LINEE GUIDA e alle POLITICHE per l’USO dell’ICT**
  e
- **COME FARE per OTTENERLE**

(nota 1: Vedi AGENZIA per l’ITALIA DIGITALE, https://www.agid.gov.it).

(nota 2: per comprendere l’IMPORTANZA …, VEDI VALORE delle INFORMAZIONI - PARTE 1_2B di Enzo Exposyto, *PAGINE da 42 a 47*.)

Torna all’INDICE

1 CONCETTI di SICUREZZA

1.3 SICUREZZA PERSONALE

1.3.1 Comprendere il termine "INGEGNERIA SOCIALE" e le sue implicazioni, quali

- **ACCESSO NON AUTORIZZATO a SISTEMI INFORMATICI,**
- **RACCOLTA NON AUTORIZZATA di INFORMAZIONI,**
- **FRODI.**

(nota 1: INGEGNERIA SOCIALE, STUDIO del COMPORTAMENTO di una PERSONA per OTTENERE INFORMAZIONI UTILI.

È UTILIZZATA soprattutto dagli HACKER -in PARTICOLARE dai CRACKER- per SCOPRIRE PASSWORD, VIOLARE SISTEMI INFORMATICI e OTTENERE DATI PERSONALI IMPORTANTI di un INDIVIDUO.)

(nota 2: per comprendere il termine "INGEGNERIA SOCIALE" …, VEDI SICUREZZA PERSONALE - PARTE 1_3 di Enzo Exposyto, *PAGINE da 12 a 26*.)

1.3.2 Identificare i METODI APPLICATI dall'INGEGNERIA SOCIALE, quali

- **CHIAMATE TELEFONICHE,**
- **PHISHING,**
- **SHOULDER SURFING (SPIARE alle SPALLE),**

al fine di CARPIRE INFORMAZIONI PERSONALI.

(nota 1: PHISHING, TIPO di TRUFFA EFFETTUATA ANCHE su INTERNET. Il MALINTENZIONATO, nelle COMUNICAZIONI con la *VITTIMA*, FINGENDOSI ESPONENTE di un ENTE AFFIDABILE e/o OPERANDO col MARCHIO dell'ENTE, la INGANNA e la CONVINCE a FORNIRE INFORMAZIONI PERSONALI, DATI FINANZIARI o CODICI di ACCESSO.)

(nota 2: per identificare i METODI APPLICATI dall'INGEGNERIA SOCIALE …, VEDI SICUREZZA PERSONALE - PARTE 1_3 di Enzo Exposyto, *PAGINE da 27 a 36*.)

Vedi pagina successiva

1 CONCETTI di SICUREZZA

1.3 SICUREZZA PERSONALE

1.3.3 Comprendere il termine "FURTO di IDENTITÀ" e le sue

- **IMPLICAZIONI PERSONALI,**
- **FINANZIARIE,**
- **LAVORATIVE,**
- **LEGALI.**

(nota: per comprendere il termine "FURTO di IDENTITÀ" …, VEDI SICUREZZA PERSONALE - PARTE 1_3 di Enzo Exposyto, *PAGINE da 37 a 39*.)

1.3.4 Identificare i METODI APPLICATI per il FURTO di IDENTITÀ, quali

- **ACQUISIRE INFORMAZIONI a partire da OGGETTI e INFORMAZIONI SCARTATI (INFORMATION DIVING);**
- **USO di DISPOSITIVI FRAUDOLENTI di LETTURA (SKIMMING);**
- **INVENTARE uno SCENARIO PRETESTUOSO (PRETEXTING).**

(nota 1: INFORMATION DIVING o, ANCHE, TRASHING)

(nota 2: accanto a SKIMMING, vedi, ANCHE WEB SKIMMING)

(nota 3: per PRETEXTING si intende, ANCHE, la CREAZIONE di SCENARI PRETESTUOSI *ONLINE* per ARRIVARE al FURTO d'IDENTITÀ.

ESEMPIO: QUALCUNO, ONLINE, *AVVISA* CHE il TUO COMPUTER HA un VIRUS.)

(nota 4: per identificare i METODI APPLICATI …, VEDI SICUREZZA PERSONALE - PARTE 1_3 di Enzo Exposyto, *PAGINE da 40 a 44*.)

Torna all'INDICE

1 CONCETTI di SICUREZZA

1.4 SICUREZZA dei FILE

1.4.1 Comprendere gli effetti di ATTIVARE/DISATTIVARE le IMPOSTAZIONI di SICUREZZA RELATIVE alle MACRO.

(nota: per comprendere gli effetti di ATTIVARE/DISATTIVARE …, VEDI SICUREZZA dei FILE - PARTE 1_4A di Enzo Exposyto, *PAGINE da 12 a 24*.)

1.4.2 Comprendere i VANTAGGI e i LIMITI della CIFRATURA.
Comprendere l'IMPORTANZA di NON DIVULGARE o di NON PERDERE

- **la PASSWORD,**
- **la CHIAVE**
  o
- **il CERTIFICATO di CIFRATURA.**

(nota 1: la CIFRATURA, in CRITTOGRAFIA, È l'OPERAZIONE con la QUALE, USANDO un CIFRARIO, SI RENDE un MESSAGGIO "OFFUSCATO", in MODO CHE NON SIA COMPRENSIBILE/INTELLIGIBILE a PERSONE NON AUTORIZZATE a LEGGERLO.)

(nota 2: per comprendere i VANTAGGI e i LIMITI della CIFRATURA …, VEDI SICUREZZA dei FILE - PARTE 1_4A di Enzo Exposyto, *PAGINE da 25 a 67*.)

Vedi pagina successiva

1 CONCETTI di SICUREZZA

1.4 SICUREZZA dei FILE

1.4.3 CIFRARE

- **un FILE,**
- **una CARTELLA,**
- **una UNITÀ DISCO.**

(nota 1: la PAGINA COME CRITTOGRAFARE (CIFRARE) un FILE della MICROSOFT INDICA, ANCHE, il *CONCRETO PROCEDIMENTO* da SEGUIRE per CRITTOGRAFARE (CIFRARE) un FILE (e NON SOLO) in RECENTI SISTEMI OPERATIVI WINDOWS.)

(nota 2: per CIFRARE …, VEDI SICUREZZA dei FILE - PARTE 1_4B di Enzo Exposyto, *PAGINE da 12 a 22*.)

1.4.4 IMPOSTARE una PASSWORD per FILE quali:

- **DOCUMENTI,**
- **FOGLI di CALCOLO,**
- **FILE COMPRESSI.**

(nota 1: la PAGINA COME PROTEGGERE un DOCUMENTO con la PASSWORD della MICROSOFT INDICA, ANCHE, il *CONCRETO PROCEDIMENTO* da SEGUIRE per IMPOSTARE una PASSWORD per FILE in RECENTI SISTEMI OPERATIVI WINDOWS.)

(nota 2: per IMPOSTARE …, VEDI SICUREZZA dei FILE - PARTE 1_4B di Enzo Exposyto, *PAGINE da 23 a 58*.)

Torna all'INDICE

2 MALWARE

2.1 TIPI e METODI

2.1.1 Comprendere il TERMINE "MALWARE".

Riconoscere DIVERSI MODI con cui il MALWARE si può nascondere nei computer, quali:

- **TROJAN,**
- **ROOTKIT**

  e
- **BACKDOOR.**

(nota 1: MALWARE, abbreviazione di MALICIOUS SOFTWARE, traducibile con SOFTWARE DANNOSO.)

(nota 2: TROJAN, tipo di MALWARE che, generalmente, SI NASCONDE all'INTERNO di un ALTRO PROGRAMMA APPARENTEMENTE UTILE e INNOCUO; vi sono DECINE di TIPI di TROJAN.)

(nota 3: ROOTKIT, collezione di SOFTWARE, tipicamente malevoli, realizzati per ACCEDERE, SENZA AUTORIZZAZIONE, a un COMPUTER o a una parte di esso.
Questi SOFTWARE, OLTRE a GARANTIRE TALI ACCESSI, MASCHERANO SÉ STESSI e/o altri programmi utili per raggiungere lo scopo.)

(nota 4: una BACKDOOR, "PORTA sul RETRO" è un METODO, SPESSO SEGRETO, per AGGIRARE, BYPASSARE, la NORMALE AUTENTICAZIONE in un SISTEMA INFORMATICO.
Ha la FUNZIONE PRINCIPALE di SUPERARE le DIFESE IMPOSTE da un SISTEMA, come può essere un FIREWALL, per ACCEDERE da REMOTO a un COMPUTER, ottenendo un'AUTENTICAZIONE che permette di prendere il COMPLETO o PARZIALE POSSESSO del DISPOSITIVO VITTIMA.)

Vedi pagina successiva

Torna all'INDICE

2 MALWARE

2.1 TIPI e METODI

2.1.2 RICONOSCERE i TIPI di MALWARE INFETTIVO e COMPRENDERE COME FUNZIONANO, ad esempio

- **VIRUS**
  e
- **WORM.**

(nota 1: VIRUS, "un VIRUS INFORMATICO è un PROGRAMMA CHE RICORSIVAMENTE ed ESPLICITAMENTE COPIA una VERSIONE POSSIBILMENTE EVOLUTA di SÉ STESSO".
I VIRUS ENTRANO nel COMPUTER SFRUTTANDO, in genere, le VULNERABILITÀ del SISTEMA OPERATIVO e ARRECANO DANNI al SISTEMA, RALLENTANDO o RENDENDO INUTILIZZABILE il DISPOSITIVO INFETTO.
I VIRUS COMPORTANO SPRECO di RISORSE in TERMINI di RAM, CPU e SPAZIO sul DISCO FISSO.)

(nota 2: un WORM, "VERME" in INGLESE, nella SICUREZZA INFORMATICA, È una PARTICOLARE CATEGORIA di MALWARE in GRADO di AUTO-REPLICARSI.
È SIMILE a un VIRUS ma, a differenza di questo, NON DEVE LEGARSI ad ALTRI PROGRAMMI ESEGUIBILI per DIFFONDERSI.
Un WORM è un PROGRAMMA per COMPUTER CHE SI REPLICA in MODO INDIPENDENTE SPEDENDOSI ad ALTRI SISTEMI e, quindi, PUÒ DIFFONDERSI MOLTO PIÙ RAPIDAMENTE.
Un WORM SI DIFFONDE, SPESSO, VIA E-MAIL.).

Vedi pagina successiva

2 MALWARE

2.1 TIPI e METODI

2.1.3 RICONOSCERE i TIPI di MALWARE USATI per

- **FURTO di DATI,**
- **PROFITTO**

  o
- **ESTORSIONE**

e comprendere COME OPERANO, ad esempio:

- **ADWARE**
  (proposta di PUBBLICITÀ attraverso BANNER e POPUP),

- **RANSOMWARE**
  (BLOCCO DOLOSO di un PROGRAMMA con lo SCOPO di CHIEDERE un RISCATTO per SBLOCCARLO),

- **SPYWARE**
  (SOFTWARE CHE INVIA ad un SERVER REMOTO i DATI di NAVIGAZIONE),

- **BOTNET**
  (SOFTWARE capace di PRENDERE il CONTROLLO di una RETE di COMPUTER),

- **KEYLOGGER**
  (SOFTWARE capace di INVIARE ad un SERVER REMOTO i CARATTERI DIGITATI su una TASTIERA)

  e
- **DIALER**
  (SOFTWARE capace di CAMBIARE la CONNESSIONE del MODEM da un PROVIDER ad un ALTRO).

Torna all'INDICE

2 MALWARE

2.2 PROTEZIONE

2.2.1 Comprendere COME FUNZIONA il SOFTWARE ANTIVIRUS e QUALI LIMITAZIONI PRESENTA.

2.2.2 Comprendere che il SOFTWARE ANTIVIRUS DOVREBBE ESSERE INSTALLATO su TUTTI i SISTEMI INFORMATICI.

2.2.3 Comprendere l'importanza di AGGIORNARE REGOLARMENTE VARI TIPI di SOFTWARE, quali:

- **ANTIVIRUS,**
- **BROWSER WEB,**
- **PLUG-IN,**
- **APPLICAZIONI,**
- **SISTEMA OPERATIVO.**

(nota: Il PLUG-IN in INFORMATICA è un PROGRAMMA *NON* AUTONOMO CHE INTERAGISCE con un ALTRO PROGRAMMA per AMPLIARNE o ESTENDERNE le FUNZIONALITÀ ORIGINARIE.
Ad ESEMPIO, un PLUG-IN per un SOFTWARE di GRAFICA PERMETTE l'UTILIZZO di NUOVE FUNZIONI NON PRESENTI nel SOFTWARE PRINCIPALE.)

2.2.4 Eseguire SCANSIONI di

- **SPECIFICHE UNITÀ,**
- **CARTELLE,**
- **FILE**

usando un SOFTWARE ANTIVIRUS.

PIANIFICARE SCANSIONI usando un SOFTWARE ANTIVIRUS.

Vedi pagina successiva

2 MALWARE

2.2 PROTEZIONE

2.2.5 Comprendere i RISCHI associati all'uso di SOFTWARE OBSOLETO e NON SUPPORTATO, quali:

- **MAGGIORI MINACCE da PARTE del MALWARE,**
- **INCOMPATIBILITÀ.**

Torna all'INDICE

2 MALWARE

2.3 RISOLUZIONE e RIMOZIONE

2.3.1 Comprendere il TERMINE "QUARANTENA" e l'EFFETTO di MESSA in QUARANTENA FILE INFETTI/SOSPETTI.

2.3.2 METTERE in QUARANTENA, ELIMINARE FILE INFETTI/SOSPETTI.

2.3.3 Comprendere che 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.**

Torna all'INDICE

3 SICUREZZA in RETE

3.1 RETI e CONNESSIONI

3.1.1 Comprendere il TERMINE "RETE" e riconoscere i PIÙ COMUNI TIPI di RETE, quali

- **LAN (rete locale),**
- **WLAN (rete locale WIRELESS),**
- **WAN (rete geografica),**
- **VPN (rete privata virtuale).**

(nota 1: LAN, LOCAL AREA NETWORK)

(nota 2: WLAN, WIRELESS LOCAL AREA NETWORK)

(nota 3: WAN, WIDE AREA NETWORK)

(nota 4: VPN, VIRTUAL PRIVATE NETWORK)

3.1.2 Comprendere che la CONNESSIONE ad una RETE HA IMPLICAZIONI di SICUREZZA, quali

- **MALWARE,**
- **ACCESSI NON AUTORIZZATI ai DATI,**
- **DIFESA della RISERVATEZZA.**

Vedi pagina successiva

3 SICUREZZA in RETE

3.1 RETI e CONNESSIONI

3.1.3 Comprendere il RUOLO dell'AMMINISTRATORE di RETE nella GESTIONE delle OPERAZIONI di

- **AUTENTICAZIONE,**
- **AUTORIZZAZIONE**

  e
- **ASSEGNAZIONE degli ACCOUNT all'INTERNO di una RETE;**
- **VERIFICA e INSTALLAZIONE di PATCH**

  e
- **AGGIORNAMENTI di SICUREZZA IMPORTANTI;**
- **CONTROLLO del TRAFFICO di RETE**

  e
- **TRATTAMENTO del MALWARE RILEVATO su una RETE.**

(nota: PATCH, "PEZZA" o "TOPPA", in INFORMATICA, INDICA una PORZIONE di SOFTWARE PROGETTATA per AGGIORNARE o MIGLIORARE un PROGRAMMA.)

3.1.4 Comprendere la FUNZIONE e i LIMITI di un FIREWALL in AMBIENTE DOMESTICO e di LAVORO.

3.1.5 ATTIVARE, DISATTIVARE un FIREWALL PERSONALE.
CONSENTIRE o BLOCCARE l'ACCESSO ATTRAVERSO un FIREWALL PERSONALE a

- **un'APPLICAZIONE,**
- **SERVIZIO**

  o
- **FUNZIONE.**

Torna all'INDICE

3 SICUREZZA in RETE

3.2 SICUREZZA su RETI WIRELESS

3.2.1 Riconoscere DIVERSI TIPI di SICUREZZA per RETI WIRELESS e i LORO LIMITI, quali:

- **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).**

3.2.2 Essere consapevoli che usando una RETE WIRELESS NON PROTETTA si va INCONTRO ad ATTACCHI da PARTE di

- **INTERCETTATORI (EAVESDROPPING),**
- **DIROTTATORI di RETE (NETWORK HIJACKING),**
- **VIOLATORI di COMUNICAZIONI PRIVATE (MAN in the MIDDLE)**

(nota 1: L'EAVESDROPPING È l'ATTO di ASCOLTARE SEGRETAMENTE o FURTIVAMENTE le CONVERSAZIONI o le COMUNICAZIONI PRIVATE di ALTRE PERSONE SENZA il LORO CONSENSO al FINE di RACCOGLIERE INFORMAZIONI.)

(nota 2: il TERMINE HIJACKING INDICA una TECNICA di ATTACCO INFORMATICO CHE CONSISTE nel MODIFICARE OPPORTUNAMENTE PACCHETTI dei PROTOCOLLI TCP/IP al FINE di *DIROTTARE* i COLLEGAMENTI ai PROPRI SITI WEB e PRENDERNE il CONTROLLO. VEDI, ANCHE, SPOOFING.)

(nota 3: lo SPOOFING È un TIPO di ATTACCO INFORMATICO che USA in VARI MODI la FALSIFICAZIONE dell'IDENTITÀ; *TO SPOOF = IMBROGLIARE*.
SPOOFING: TIPO di COMPORTAMENTO con CUI un HACKER/CRACKER FINGE di ESSERE ALTRO UTENTE o SIMULA un DISPOSITIVO ATTENDIBILE PERCHÉ la VITTIMA FACCIA QUALCOSA a VANTAGGIO dell'HACKER/CRACKER; ESEMPI: *EMAIL SPOOFING* e *IP SPOOFING*)

(nota 4: ATTACCO "MAN in the MIDDLE", "UOMO nel MEZZO", in CRITTOGRAFIA e in SICUREZZA INFORMATICA, indica un ATTACCO INFORMATICO in cui QUALCUNO SEGRETAMENTE RITRASMETTE o ALTERA la COMUNICAZIONE tra DUE PARTI CHE CREDONO di COMUNICARE DIRETTAMENTE tra LORO.)

Vedi pagina successiva

Torna all'INDICE

3 SICUREZZA in RETE

3.2 SICUREZZA su RETI WIRELESS

3.2.3 Comprendere il TERMINE "HOTSPOT PERSONALE".

(nota: VEDI ANCHE HOTSPOT MOBILE, TETHERING e ACCESS POINT)

3.2.4 ATTIVARE, DISATTIVARE un HOTSPOT PERSONALE SICURO, CONNETTERE in MODO SICURO e DISCONNETTERE DISPOSITIVI INFORMATICI.

Torna all'INDICE

4 CONTROLLO di ACCESSO

4.1 METODI

4.1.1 Identificare i METODI per IMPEDIRE ACCESSI NON AUTORIZZATI ai DATI, quali:

- **NOME UTENTE,**
- **PASSWORD,**
- **PIN,**
- **CIFRATURA,**
- **AUTENTICAZIONE a PIÙ FATTORI.**

(nota: PIN, PERSONAL IDENTIFICATION NUMBER.)

4.1.2 Comprendere il termine "ONE-TIME PASSWORD" e il SUO UTILIZZO TIPICO.

(nota: ONE-TIME PASSWORD, OTP.)

4.1.3 Comprendere lo SCOPO di un ACCOUNT di RETE.

4.1.4 Comprendere
che per ACCEDERE alla RETE SONO NECESSARI

- **un NOME UTENTE**
  e
- **una PASSWORD,**

e che È IMPORTANTE DISCONNETTERE l'ACCOUNT, al TERMINE del COLLEGAMENTO.

4.1.5 Identificare le COMUNI TECNICHE di SICUREZZA BIOMETRICA usate per il CONTROLLO degli ACCESSI, quali

- **IMPRONTE DIGITALI,**
- **SCANSIONE dell'OCCHIO,**
- **RICONOSCIMENTO FACCIALE,**
- **GEOMETRIA della MANO**

Torna all'INDICE

4 CONTROLLO di ACCESSO

4.2 GESTIONE delle PASSWORD

4.2.1 Riconoscere BUONE LINEE di CONDOTTA per la PASSWORD, quali

- **SCEGLIERE le PASSWORD di LUNGHEZZA ADEGUATA**
  e
- **CONTENENTI un NUMERO SUFFICIENTE di**
- **LETTERE,**
- **NUMERI**
  e
- **CARATTERI SPECIALI;**
- **EVITARE di CONDIVIDERLE,**
- **MODIFICARLE con REGOLARITÀ,**
- **SCEGLIERE PASSWORD DIVERSE per servizi diversi.**

4.2.2 Comprendere la FUNZIONE e le LIMITAZIONI dei SOFTWARE di GESTIONE delle PASSWORD.

Torna all'INDICE

5 USO SICURO del WEB

5.1 IMPOSTAZIONI del BROWSER

5.1.1 SELEZIONARE IMPOSTAZIONI ADEGUATE per ATTIVARE, DISATTIVARE

- **il COMPLETAMENTO AUTOMATICO,**
- **il SALVATAGGIO AUTOMATICO**

QUANDO si COMPILA un MODULO.

5.1.2 ELIMINARE DATI PRIVATI da un BROWSER, quali

- **CRONOLOGIA di NAVIGAZIONE,**
- **CRONOLOGIA di SCARICAMENTO,**
- **FILE TEMPORANEI di INTERNET,**
- **PASSWORD,**
- **COOKIE,**
- **DATI per il COMPLETAMENTO AUTOMATICO.**

Torna all'INDICE

5 USO SICURO del WEB

5.2 NAVIGAZIONE SICURA in RETE

5.2.1 ESSERE CONSAPEVOLI CHE ALCUNE ATTIVITÀ in RETE (ACQUISTI, TRANSAZIONI FINANZIARIE) DEVONO ESSERE ESEGUITE

- **SOLO SU PAGINE WEB SICURE**
  e
- **con l'USO di una CONNESSIONE di RETE SICURA.**

5.2.2 Identificare le MODALITÀ con CUI CONFERMARE la AUTENTICITÀ di un SITO WEB, quali:

- **QUALITÀ DEL CONTENUTO,**
- **ATTUALITÀ,**
- **VALIDITÀ URL,**
- **INFORMAZIONI sulla SOCIETÀ o sul PROPRIETARIO,**
- **INFORMAZIONI di CONTATTO,**
- **CERTIFICATO di SICUREZZA,**
- **VALIDAZIONE del PROPRIETARIO del DOMINIO.**

5.2.3 Comprendere il TERMINE "PHARMING".

(nota: PHARMING, REDIRECTING to FRAUDULENT WEBSITES.
In ambito informatico, si definisce PHARMING una TECNICA di CRACKING, UTILIZZATA per OTTENERE l'ACCESSO ad INFORMAZIONI PERSONALI e RISERVATE, con varie finalità.
Grazie a questa tecnica, l'UTENTE È INGANNATO e PORTATO a RIVELARE INCONSAPEVOLMENTE a SCONOSCIUTI i PROPRI DATI SENSIBILI, come NUMERO di CONTO CORRENTE, NOME UTENTE, PASSWORD, NUMERO di CARTA di CREDITO, et cetera)

Vedi pagina successiva

5 USO SICURO del WEB

5.2 NAVIGAZIONE SICURA in RETE

5.2.4 Comprendere la FUNZIONE e i TIPI di SOFTWARE per il CONTROLLO del CONTENUTO, quali

- **SOFTWARE per il FILTRAGGIO di INTERNET,**
- **SOFTWARE di CONTROLLO GENITORI.**

Torna all'INDICE

6 COMUNICAZIONI

6.1 POSTA ELETTRONICA

6.1.1 Comprendere lo SCOPO di CIFRARE, DECIFRARE un MESSAGGIO di POSTA ELETTRONICA.

6.1.2 Comprendere il TERMINE "FIRMA DIGITALE".

(nota: in ITALIA, la FIRMA DIGITALE è DISCIPLINATA dal CODICE dell'AMMINISTRAZIONE DIGITALE, in PARTICOLARE dall'ARTICOLO 24.
COME RIPORTA WIKIPEDIA, la FIRMA DIGITALE È un METODO MATEMATICO per AUTENTICARE l'AUTORE di un DOCUMENTO DIGITALE e DIMOSTRARE l'AUTENTICITÀ del DOCUMENTO.)

6.1.3 IDENTIFICARE i POSSIBILI MESSAGGI FRAUDOLENTI o INDESIDERATI.

6.1.4 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.**

6.1.5 Essere CONSAPEVOLI CHE È POSSIBILE DENUNCIARE TENTATIVI di PHISHING

- **alle ORGANIZZAZIONI COMPETENTI**
  o
- **alle AUTORITÀ PREPOSTE.**

6.1.6 Essere CONSAPEVOLI del RISCHIO di INFETTARE un COMPUTER o un DISPOSITIVO con MALWARE attraverso l'APERTURA di

- **un ALLEGATO CONTENENTE una MACRO**
  o
- **un FILE ESEGUIBILE.**

Torna all'INDICE

6 COMUNICAZIONI

6.2 RETI SOCIALI

6.2.1 Comprendere l'IMPORTANZA di NON DIVULGARE su SITI di RETI SOCIALI INFORMAZIONI RISERVATE o INFORMAZIONI PERSONALI CHE PERMETTONO l'IDENTIFICAZIONE.

6.2.2 Essere CONSAPEVOLI della NECESSITÀ di APPLICARE e di RIVEDERE con REGOLARITÀ le IMPOSTAZIONI del PROPRIO ACCOUNT su una RETE SOCIALE, quali

- **RISERVATEZZA dell'ACCOUNT**
  e
- **PROPRIA POSIZIONE.**

6.2.3 APPLICARE le IMPOSTAZIONI degli ACCOUNT di RETI SOCIALI:

- **RISERVATEZZA dell'ACCOUNT**
  e
- **PROPRIA POSIZIONE.**

6.2.4 Comprendere i 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.**

(nota: CHILD GROOMING, ADESCAMENTO di MINORI)

Vedi pagina successiva

Torna all'INDICE

6 COMUNICAZIONI

6.2 RETI SOCIALI

6.2.5 Essere CONSAPEVOLI CHE È POSSIBILE DENUNCIARE USI o COMPORTAMENTI INAPPROPRIATI della RETE SOCIALE

- **al FORNITORE del SERVIZIO**
  o
- **alle AUTORITÀ PREPOSTE.**

Torna all'INDICE

6 COMUNICAZIONI

6.3 VoIP e MESSAGGISTICA ISTANTANEA

6.3.1 Comprendere le VULNERABILITÀ di SICUREZZA della MESSAGGISTICA ISTANTANEA e del VoIP (VOICE over INTERNET PROTOCOL), quali

- **MALWARE,**
- **ACCESSO da BACKDOOR,**
- **ACCESSO a FILE,**
- **INTERCETTAZIONE (EAVESDROPPING).**

(nota 1: una BACKDOOR, "PORTA sul RETRO" è un METODO, SPESSO SEGRETO, per AGGIRARE, BYPASSARE, la NORMALE AUTENTICAZIONE in un SISTEMA INFORMATICO.
Ha la FUNZIONE PRINCIPALE di SUPERARE le DIFESE IMPOSTE da un SISTEMA, come può essere un FIREWALL, per ACCEDERE da REMOTO a un COMPUTER, ottenendo un'AUTENTICAZIONE che permette di prendere il COMPLETO o PARZIALE POSSESSO del DISPOSITIVO VITTIMA.)

(nota2: EAVESDROPPING, ASCOLTARE di NASCOSTO, ORIGLIARE.
Vedi ANCHE SNIFFING: FIUTARE, ANNUSARE.
Vedi, INOLTRE, SNOOPING: FARE il FICCANASO, SPIARE, CURIOSARE.)

[nota 3: SNIFFING, ODORARE in Inglese, sia in INFORMATICA sia nelle TELE-COMUNICAZIONI, definisce l'ATTIVITÀ di INTERCETTAZIONE PASSIVA dei DATI CHE TRANSITANO in una RETE TELEMATICA.
TALE ATTIVITÀ PUÒ ESSERE SVOLTA

- **sia per SCOPI LEGITTIMI (ad esempio, l'INDIVIDUAZIONE di PROBLEMI di COMUNICAZIONE o di TENTATIVI di INTRUSIONE)**
- **sia per SCOPI ILLECITI (INTERCETTAZIONE FRAUDOLENTA di PASSWORD o ALTRE INFORMAZIONI SENSIBILI).]**

(nota 4: SECONDO it.wiktionary.org, SNOOPING, in INFORMATICA, È PRENDERE il CONTROLLO dell'IDENTITÀ o del PROFILO di un'ALTRA PERSONA. Lo SNOOPING è USATO, anche, dagli AMMINISTRATORI dei PORTALI quando essi ACCEDONO con l'IDENTITÀ di un UTENTE per MODIFICARE DATI o RIMUOVERE CONTENUTI INAPPROPRIATI.)

Vedi pagina successiva

Torna all'INDICE

6 COMUNICAZIONI

6.3 VoIP e MESSAGGISTICA ISTANTANEA

6.3.2 Riconoscere i METODI per ASSICURARE la CONFIDENZIALITÀ DURANTE l'USO della MESSAGGISTICA ISTANTANEA e del VoIP (VOICE over INTERNET PROTOCOL), quali

- **CIFRATURA,**
- **NON DIVULGAZIONE di INFORMAZIONI IMPORTANTI,**
- **LIMITAZIONE alla CONDIVISIONE di FILE.**

Torna all'INDICE

6 COMUNICAZIONI

6.4 DISPOSITIVI MOBILI

6.4.1 Comprendere le POSSIBILI 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.**

(nota: a PARTE gli ALTRI POSSIBILI GRAVI DANNI all'UTENTE, TALE TIPO di APPLICAZIONI *PUÒ UTILIZZARE RISORSE NON NECESSARIE*.)

6.4.2 Comprendere il TERMINE "AUTORIZZAZIONI dell'APPLICAZIONE".

(nota: le AUTORIZZAZIONI CHIESTE dalle APP POSSONO FORNIRE ad ESSE il CONTROLLO del TUO DISPOSITIVO e l'ACCESSO a FOTOCAMERA, MICROFONO, CONVERSAZIONI e MESSAGGI PRIVATI, FOTO RISERVATE e MOLTO ALTRO.
QUESTE RICHIESTE VENGONO VISUALIZZATE la PRIMA VOLTA che un'APP DEVE ACCEDERE ad HARDWARE o a DATI SENSIBILI sul TUO DEVICE e IN GENERE RIGUARDANO la PRIVACY.)

Vedi pagina successiva

6 COMUNICAZIONI

6.4 DISPOSITIVI MOBILI

6.4.3 Essere CONSAPEVOLI che le APPLICAZIONI MOBILI POSSONO ESTRARRE INFORMAZIONI PRIVATE dal DISPOSITIVO MOBILE, quali

- **DETTAGLI dei CONTATTI,**
- **CRONOLOGIA delle POSIZIONI,**
- **IMMAGINI.**

(nota: a PARTE la POSSIBILITÀ CHE ESTRAGGANO ALTRE INFORMAZIONI PRIVATE dell'UTENTE, le APPLICAZIONI MOBILI POSSONO ESTRARRE i *DETTAGLI dei CONTATTI*.)

6.4.4 Essere CONSAPEVOLI delle 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.**

Torna all'INDICE

7 GESTIONE SICURA dei DATI

7.1 MESSA in SICUREZZA e SALVATAGGIO di DATI

7.1.1 Riconoscere i MODI per ASSICURARE la SICUREZZA FISICA di COMPUTER e DISPOSITIVI MOBILI, quali

- **NON LASCIARLI INCUSTODITI,**
- **REGISTRARE la COLLOCAZIONE**
  e
- **i DETTAGLI degli APPARATI,**
- **USARE CAVI ANTIFURTO,**
- **CONTROLLARE gli ACCESSI alle SALE dei COMPUTER.**

7.1.2 Riconoscere l'IMPORTANZA di AVERE una PROCEDURA di COPIE di SICUREZZA per OVVIARE alla PERDITA di DATI da COMPUTER e da DISPOSITIVI MOBILI.

7.1.3 Identificare le CARATTERISTICHE di una PROCEDURA di COPIE di SICUREZZA, quali

- **REGOLARITÀ/FREQUENZA,**
- **PIANIFICAZIONE,**
- **COLLOCAZIONE del SUPPORTO dei DATI SALVATI,**
- **COMPRESSIONE dei DATI.**

7.1.4 EFFETTUARE la COPIA di SICUREZZA di DATI su un SUPPORTO quale:

- **UNITÀ DISCO**
  o
- **DISPOSITIVO LOCALE,**
- **UNITÀ ESTERNA,**
- **SERVIZIO su CLOUD.**

Vedi pagina successiva

7 GESTIONE SICURA dei DATI

7.1 MESSA in SICUREZZA e SALVATAGGIO di DATI

7.1.5 RIPRISTINARE i DATI da una COPIA di SICUREZZA su

- **UNITÀ DISCO**
  o
- **DISPOSITIVO LOCALE,**
- **UNITÀ ESTERNA,**
- **SERVIZIO su CLOUD.**

Torna all'INDICE

7 GESTIONE SICURA dei DATI

7.2 CANCELLAZIONE e DISTRUZIONE SICURA

7.2.1 DISTINGUERE tra

- **CANCELLARE i DATI**
  ed
- **ELIMINARLI in MODO PERMANENTE.**

7.2.2 Comprendere i MOTIVI per ELIMINARE in MODO PERMANENTE i DATI dalle MEMORIE di MASSA o dai DISPOSITIVI MOBILI.

7.2.3 Essere CONSAPEVOLI CHE l'ELIMINAZIONE del CONTENUTO dai SERVIZI POTREBBE NON ESSERE PERMANENTE, come nel caso dei

- **SITI di RETI SOCIALI,**
- **BLOG,**
- **FORUM su INTERNET,**
- **SERVIZI su CLOUD.**

7.2.4 Identificare i METODI PIÙ COMUNI per DISTRUGGERE i DATI in MODO PERMANENTE, quali

- **USO di TRITA DOCUMENTI,**
- **DISTRUZIONE di MEMORIE di MASSA**
  o
- **DISPOSITIVI,**
- **SMAGNETIZZAZIONE,**
- **USO di SOFTWARE per la CANCELLAZIONE DEFINITIVA dei DATI.**

Torna all'INDICE