



## ***CYBER SECURITY AWARENESS***

### ***LA CULTURA DELLA SICUREZZA INFORMATICA***

***Brescia, 7 Marzo 2023***



## Argomenti

- ★ **LA CULTURA DELLA CYBER SICUREZZA**
- ★ **ALCUNI DATI AL RIGUARDO ...**
- ★ **MINACCE ALLA SICUREZZA**



# LA CULTURA DELLA CYBER SICUREZZA

## LA CULTURA DELLA CYBER SICUREZZA (CYBER SECURITY AWARENESS)

### NIST Special Publication 800-16

Awareness is not training. The purpose of awareness presentations is simply to focus attention on security and understand why security is important. Awareness presentation are intended to allow individuals to recognize IT security concerns and respond accordingly.

- SCOPO DI QUESTE PRESENTAZIONI È PORRE L'ATTENZIONE SULLA CULTURA DELLA SICUREZZA, CONCETTO DIVERSO DALLA FORMAZIONE, ENFATIZZANDONE L'IMPORTANZA.
- IL NOSTRO CONTRIBUTO È MIRATO AD INDIVIDUARE LE CRITICITÀ DELLA SICUREZZA DEL DATO DIGITALE E LE APPROPRIATE RISPOSTE.



FONTE: [https://securitymea.com/wp-content/uploads/2019/11/Security-Awareness\\_2.jpg](https://securitymea.com/wp-content/uploads/2019/11/Security-Awareness_2.jpg)

LA SECURITY AWARENESS CONSISTE NEL RENDERE LE PERSONE E LE ORGANIZZAZIONI CONSAPEVOLI DELLE ATTUALI MINACCE INFORMATICHE E GLI STRUMENTI ADATTI PER PREVENIRE, RICONOSCERE E REAGIRE AGLI INCIDENTI INFORMATICI (DATA BREACH).



# LA CULTURA DELLA CYBER SICUREZZA

IL DIGITALE È DIVENTATO CENTRALE PER LA  
IL FUNZIONAMENTO DI AZIENDE E  
PUBBLICHE AMMINISTRAZIONI

QUANTO SIETE CONSAPEVOLI DEI RISCHI SULLA SICUREZZA IN  
AMBITO CYBER NELLA VOSTRA ORGANIZZAZIONE ?



NON ESISTE DIGITALIZZAZIONE POSSIBILE SENZA SICUREZZA



# LA CULTURA DELLA CYBER SICUREZZA

## LA CENTRALITÀ DELLA PERSONA NELLA CYBERSECURITY

LA RESILIENZA (O LA FRAGILITÀ) DI UN SISTEMA DI CYBER SECURITY  
È FORTEMENTE DETERMINATA DAL FATTORE UMANO:  
OCCORRE INVESTIRE SULLA PERSONA , SULLA SUA FORMAZIONE E IL  
SUO AGGIORNAMENTO !!!

+ CONOSCENZA

E

=

+ CONSAPEVOLEZZA

+ ESPERIENZA

LA SICUREZZA ASSOLUTA NON ESISTE !!! ESISTONO SOLO DEI COMPORTAMENTI,  
DELLE PROCEDURE, DEI PIANI DI AZIONE, DELLE SOLUZIONI DA ADOTTARE NEL  
QUOTIDIANO PER RIDURRE IL RISCHIO DI ATTACCHI INFORMATICI



# LA CULTURA DELLA CYBER SICUREZZA

## PERCHÉ È FONDAMENTALE CAPIRE CHE I NOSTRI DATI SONO UN PATRIMONIO DI VITALE IMPORTANZA ... ?

- I DATI SONO IL CORE BUSINESS DI GRAN PARTE DELLE ORGANIZZAZIONI E I SERVIZI DA ESSE EROGATI SI BASANO PROPRIO SULLA RACCOLTA E SULLA ELABORAZIONE DI QUESTI DATI
- I DATI PERSONALI QUALORA VENISSERO CARPITI, DIVULGATI E UTILIZZATI DA MALINTENZIONATI POTREBBERO LEDERE LA RISERVATEZZA E LA DIGNITÀ DI TALI PERSONE OLTRE CHE L'ORGANIZZAZIONE STESSA A CUI APPARTENGONO
- LA GESTIONE DEI DATI È SOTTOPOSTA A DISCIPLINE NORMATIVE. È NECESSARIO PRESTARE PARTICOLARE ATTENZIONE ALLA GESTIONE DEI COSIDDETTI DATI SENSIBILI PENA L'INCORRERE IN SANZIONI



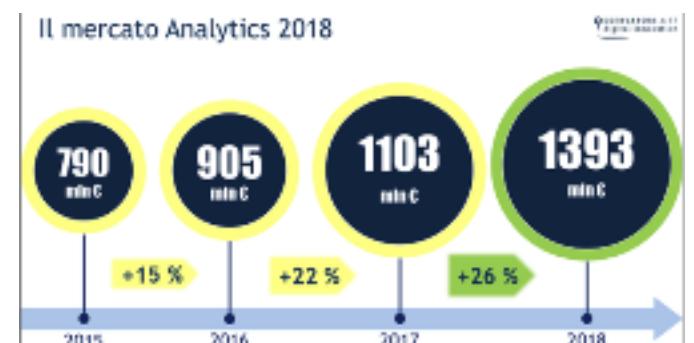
FONTE: <https://3rdplace.com/news/data-driven-strategy-l-importanza-dei-dati/>

## BIG DATA



FONTE: <https://www.sadasdb.com/cosa-sono-big-data-quale-vantaggi-per-aziende/>

**I DATI SONO IMPORTANTI  
E PRODUCONO VALORE**



FONTE: <https://www.bigdata4innovation.it/big-data/big-data-analytics-in-italia/>



# LA CULTURA DELLA CYBER SICUREZZA

- GLI ATTACCHI INFORMATICI SONO MIRATI ...
- LA MIA ORGANIZZAZIONE NON È A RISCHIO PERCHE' I MIEI DATI NON SONO APPETIBILI...
- NON SERVE INVESTIRE IN CYBER SICUREZZA ...

***NIENTE DI PIÙ SBAGLIATO !!!***



**PERCHÉ IN REALTÀ ...**

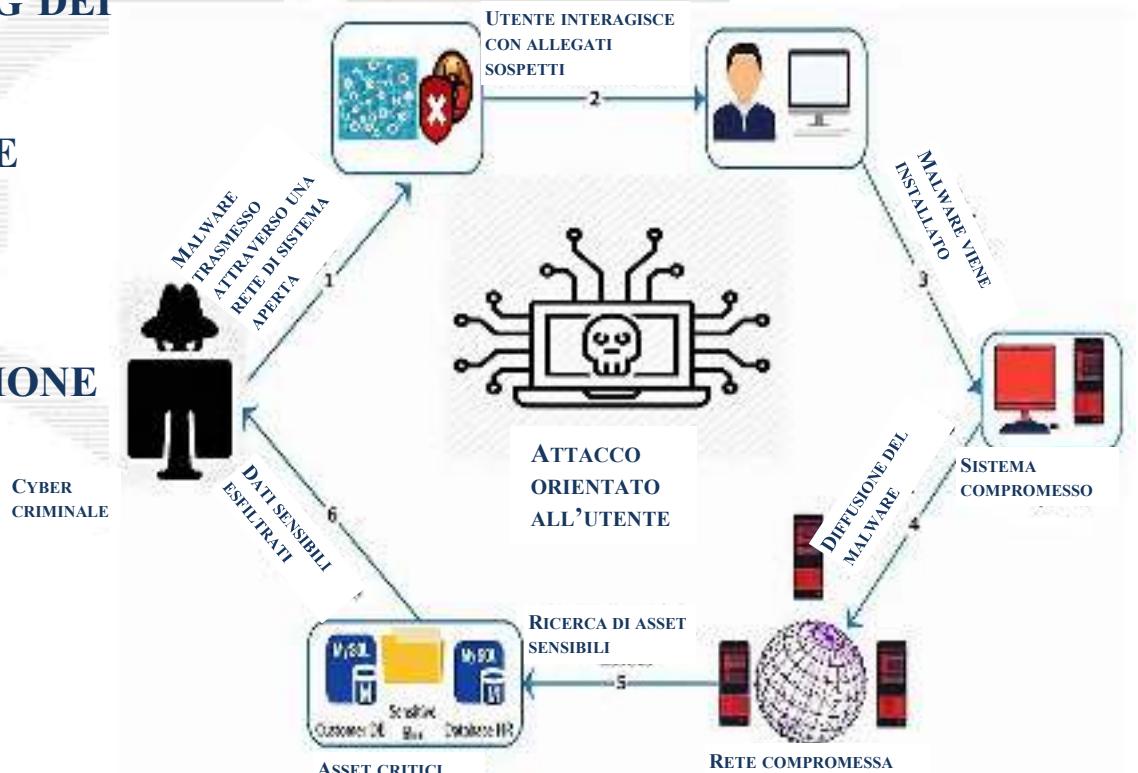
- MOLTI ATTACCHI INFORMATICI MIRANO AD UN NUMERO ELEVATO DI ORGANIZZAZIONI
- I NOSTRI DATI SONO IMPORTANTI PER NOI E LA LORO INDISPONIBILITÀ O PUBBLICAZIONE POSSONO COMPORTARE COSTI MOLTO SIGNIFICATIVI



# LA CULTURA DELLA CYBER SICUREZZA

**SONO DIVERSI I FATTORI CHE BISOGNA TENERE IN CONSIDERAZIONE  
QUANDO SI HA A CHE FARE CON LA CYBER SICUREZZA ...**

- **LE DEBOLEZZE DEL COMPORTAMENTO UMANO (ABITUDINARIETÀ, TENDENZA A FIDARSI, SUPERFICIALITÀ, AVVERSIONE VERSO LE RESTRIZIONI)**
- **CAPACITÀ DI SOCIAL ENGINEERING DEI POSSIBILI ATTACCANTI**
- **LA TIPOLOGIA DI ORGANIZZAZIONE**
- **LA TIPOLOGIA DEI DATI GESTITI**
- **LE TECNOLOGIE IN USO**
- **RISORSE ECONOMICHE A DISPOSIZIONE**
- **ECC...**



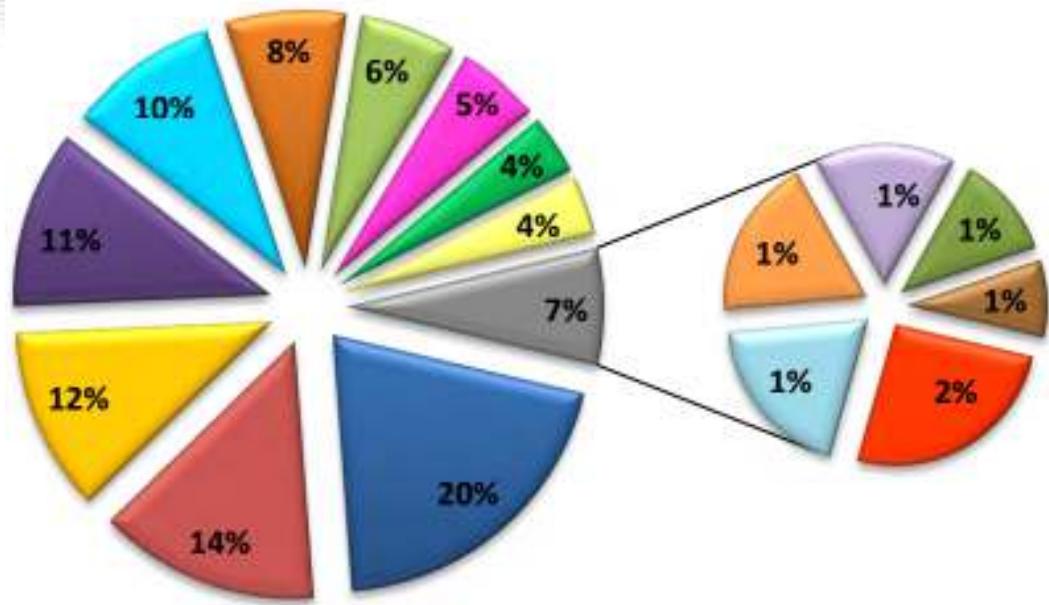


# LA CULTURA DELLA CYBER SICUREZZA

## ALCUNI DATI AL RIGUARDO ...

- GLI ATTACCHI INFORMATICI RIGUARDANO ORGANIZZAZIONI DI OGNI TIPO
- IL SOLO FATTO CHE UN SISTEMA INFORMATICO SIA CONNESSO ALLA RETE INTERNET COMPORTA RISCHI PER LA SICUREZZA

Tipologia e distribuzione delle vittime (2020)



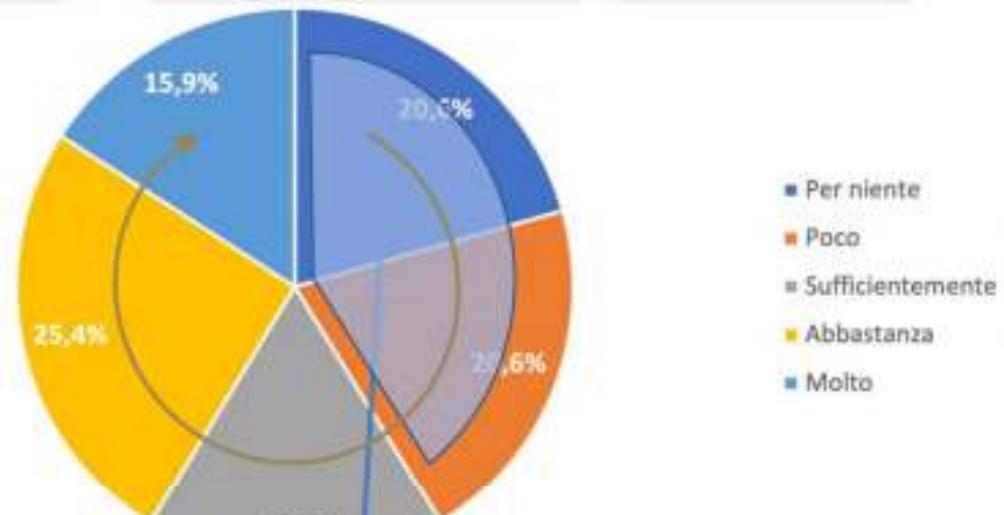
- TARGET MULTIPLI
- GOVERNO, FORZE ARMATE, FORZE DELL'ORDINE, SERVIZI E INTELLIGENCE
- SALUTE/SANITÀ
- ISTRUZIONE E RICERCA
- SERVIZI ONLINE, CLOUD
- ALTRI
- FORNITORI DI SOFTWARE E HARDWARE
- MONDO BANCARIO E DELLA FINANZA
- INFRASTRUTTURE CRITICHE (CENTRALI ELETTRICHE, IDRICHE, NUCLEARI, ...)
- INTRATTENIMENTO E INFORMAZIONE
- GRANDE DISTRIBUZIONE ORGANIZZATA E VENDITA AL DETTAGLIO
- ORGANIZZAZIONI NON GOVERNATIVE
- COMPAGNIE DI TELECOMUNICAZIONI
- TURISMO E RELAX
- APPALTATORI E CONSULENZE GOVERNATIVE
- SICUREZZA

## ALCUNI DATI AL RIGUARDO ...

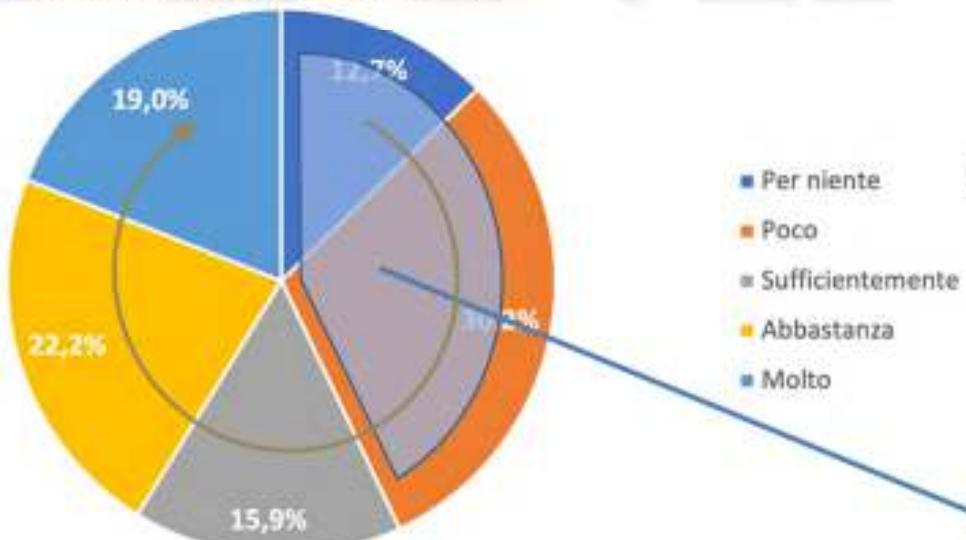
### ATTACCO INFORMATICO



### CAPACITÀ DI DIFESA



### CONSAPEVOLEZZA SUI RISCHI



*Ripartizione del campione per capacità di difesa da attacchi informatici*

C'È ANCORA UNA FETTA AMPIA DI ORGANIZZAZIONI E PERSONE CHE HANNO SCARSE CAPACITÀ DI DIFENDERSI DA ATTACCHI INFORMATICI.

*Ripartizione del campione intervistato per grado di consapevolezza sui rischi conseguenti un attacco*

C'È ANCORA UNA FETTA AMPIA DI ORGANIZZAZIONI E PERSONE CHE NON SANNO A QUALI RISCHI VANNO INCONTRO NEL CASO VENGANO COLPITI DA ATTACCHI INFORMATICI.



# LA CULTURA DELLA CYBER SICUREZZA

CARABINIERI

## MINACCE ALLA SICUREZZA

OGGI LA SICUREZZA INFORMATICA È MESSA ALLA PROVA DA VARI PERICOLI. NON SI PARLA PIÙ DI SEMPLICI HACKER MA DI VERE E PROPRIE ORGANIZZAZIONI CRIMINALI BEN STRUTTURATE E CON MOLTE RISORSE PER RAGGIUNGERE I LORO SCOPI





# LA CULTURA DELLA CYBER SICUREZZA

## RANSOMWARE

- IL RANSOMWARE È UN TIPO DI SOFTWARE MALEVOLO (MALWARE) CHE CRITTOGRAFA DOCUMENTI, IMMAGINI E ALTRI FILE, RENDENDOLI INUTILIZZABILI
- LA CHIAVE DI DECRITTAZIONE VIENE FORNITA SOLO A FRONTE DEL PAGAMENTO DI UN RISCATTO, DI NORMA IN CRIPTO VALUTA (E.G. BITCOIN)
- POICHÉ UN METODO PER PROTEGGERSI È EFFETTUARE REGOLARI BACKUP DEI DATI, LE NUOVE VERSIONI DI RANSOMWARE PROVVEDONO ANCHE ALL'ESFILTRAZIONE DEI DATI. LA MINACCIA DELLA PUBBLICAZIONE COSTITUISCE UN ULTERIORE ELEMENTO DI PRESSIONE SULLA VITTIMA

I VETTORI DI INFESTAZIONE TIPICI DEI RANSOMWARE SONO:

- INVIO DI EMAIL CONTENENTI ALLEGATI INFETTI O COLLEGAMENTI A SITI ESTERNI
- NAVIGAZIONE SU SITI COMPROMESSI
- VULNERABILITÀ DELLA RETE AZIENDALE





# LA CULTURA DELLA CYBER SICUREZZA

## RANSOMWARE

Your computer has been infected



Your documents, photos, databases and other important files encrypted



To decrypt your files you need to buy our special software - Decryptor



Follow the instructions below. But remember that you do not have much time

-Decryptor price

You have **1 day, 23:59:04**

\* If you do not pay on time, the price will be doubled.  
\* Time ends on Feb 14, 07:50:33

Monero address: 0000000000000000000000000000000000000000000000000000000000000000

Current price

After time ends

**963.436 XMR**

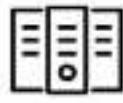
= 200,000 USD

**1926.072 XMR**

= 400,000 USD



Your network has been infected!



Your documents, photos, databases and other important files encrypted



To decrypt your files you need to buy our special software - General-Decryptor



Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

You have **11 days, 02:23:24**

\* If you do not pay on time, the price will be doubled  
\* Time ends on Feb 23, 23:38:44

Monero address: 0000000000000000000000000000000000000000000000000000000000000000

INSTRUCTIONS

CHAT SUPPORT

ABOUT US

Current price

After time ends

**10109.68 XMR**

= 2,000,000 USD

**20219.36 XMR**

= 4,000,000 USD

(1) Riscatto Sodinokibi solo cifratura file  
Fonte: CRAM di TG Soft

(2) Riscatto Sodinokibi cifratura+esfiltrazione file - Fonte: CRAM di TG Soft

**RISCATTO MOLTO SALATO**

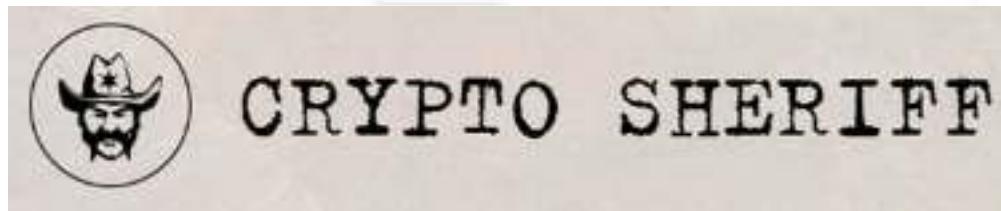


# LA CULTURA DELLA CYBER SICUREZZA

## RANSOMWARE

**PAGARE IL RISCATTO NON È MAI CONSIGLIABILE**

- **NON SI HA ALCUNA CERTEZZA DI OTTENERE LA CHIAVE DI DECIFRATURA**
- **SI INCORAGGIANO ANALOGHE AZIONI VERSO ALTRI MALCAPITATI**
- **A VOLTE È POSSIBILE AIUTARE LE VITTIME A RIOTTENERE L'ACCESSO AI PROPRI FILE CRIPTATI SENZA DOVER PAGARE NULLA. ESISTONO DATABASE DELLE CHIAVI CHE SONO IN GRADO DI DECRYPTARE I DATI COLPITI DA DIVERSI TIPI DI RANSOMWARE ([WWW.NOMORERANSOM.ORG](http://www.nomoreransom.org))**



FONTE: <https://www.secplicity.org/2016/07/28/ransomware-call-in-a-crypto-sheriff/>



FONTE: <https://news.softpedia.com/news/id-ransomware-website-helps-identify-ransomware-infections-502814.shtml>



# LA CULTURA DELLA CYBER SICUREZZA

## PHISHING

IL PHISHING È UN TIPO DI TRUFFA ATTRAVERSO LA QUALE UN MALINTENZIONATO CERCA DI INGANNARE LA VITTIMA CONVINCENDOLA A FORNIRE INFORMAZIONI PERSONALI, DATI FINANZIARI O CODICI DI ACCESSO, FINGENDOSI PARTE AFFIDABILE IN UNA COMUNICAZIONE DIGITALE.

LE PIÙ COMUNI TECNICHE DI PHISHING MIRANO AD INDURRE LA VITTIMA A COMUNICARE I PROPRI DATI E CREDENZIALI PERSONALI IN SITI WEB CHE ASSOMIGLIANO A QUELLI LEGITTIMI, PER ESEMPIO:

- UN'AZIONE RICHIESTA COME PARTE DI UN AGGIORNAMENTO DEL SISTEMA
- UN'AZIONE NECESSARIA PER IMPEDIRE LA CHIUSURA DELL'ACCOUNT E-MAIL
- UN FORNITORE AFFIDABILE, COME DROPBOX O UN AVVISO DI GOOGLE
- UN AVVISO DELLA BANCA CHE INVITA A CAMBIARE LA PASSWORD IN SCADENZA

I PHISHER UTILIZZANO L'IDENTITÀ DELLA VITTIMA PER INDURRE ALTRI IN ERRORE O ACQUISTARE BENI O SERVIZI





# LA CULTURA DELLA CYBER SICUREZZA

## PHISHING



- Campagna di phishing che si spaccia per OMS. Fonte: Libraesva



# LA CULTURA DELLA CYBER SICUREZZA

## PHISHING

Ds: Telecom Italia-TIM 1493615864clientiservizio@tim1493615864.it  
Oggetto: Fattura TIM linea Fissa - Maggio 2017 - scadenza 01/05/2017

11/05/2017 07:14

**TELECOM** **TIM**

Gentile cliente,

ti informiamo che la tua fattura TIM di Maggio 2017 relativa alla linea Fattura 00726377-288389 è stata appena emessa ed è disponibile online.

**Si prega di scaricare il fattura attaccato**

Ti ricordiamo che in MyTIM Fisso nella sezione Il mio profilo puoi richiedere di ricevere la fattura TIM esclusivamente online. Risparmierai così le spese di spedizione postale.

Ti aspettiamo presto su [www.tim.it](http://www.tim.it)

Grazie

Servizio Clienti tim.it

**1 allegato: Fattura 00726377-288389.pdf**

Da: Cristina Eugignani <office@app.income.com>  
Oggetto: Fattura 01/05 - ddt Applicazioni Tecniche srl

11/05/2017 11:11

Ringraziare la ricevuta eci tecniche ci cura 7.5.C consente a salvo della lettura 37.C  
nel tempo che ci pari importante.  
Cordiali saluti.

Cristina Eugignani  
Ufficio Clienti Italia - DDT Applicazioni Tecniche srl  
Tel. +39.651.776336  
Fax. +39.06.776336

This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: PayPal [service@paypal-australia.com.au]  
To: **[REDACTED]**  
Cc:  
Subject: Your account has been limited

Thu 28.06.2012 0:24 AM

**1. Finto dominio**

**2. Oggetto e contenuto sospetti**

**3. Errore grammaticale**

**4. Link sospetti**

**PayPal**

How to restore your PayPal account

Dear PayPal member,  
To restore your PayPal account, you'll need to **log in** to your account.

It's easy:

1. Click on the link below to open a secure browser window.
2. Confirm <http://69.162.70.169/ppau/> the account, and then follow the instructions.

**Log in your account now**

PayPal Email ID PP32260008777626



# LA CULTURA DELLA CYBER SICUREZZA

## VIRUS E MALWARE

- I MALWARE POSSONO ACQUISIRE TUTTO CIÒ CHE SI SCRIVE SULLA TASTIERA (KEYLOGGING), CONTROLLARE LA WEBCAM/MICROFONO, ESFILTRARE FILE ED INVIARE I DATI A SERVER REMOTI
- SPESO SONO CONTENUTI IN ALLEGATI IN FORMATO WORD, EXCEL O PDF CHE DEVONO ESSERE APERTI PRIMA CHE IL MALWARE SI ATTIVI.
- SPESO I MALWARE TRAGGONO VANTAGGIO DAI SOFTWARE O SISTEMI OPERATIVI NON AGGIORNATI
- ALCUNI MALWARE RICHIEDONO L'ABILITAZIONE DELLE MACRO: SOSPIETTARE SEMPRE DI UN ALLEGATO CHE RICHIENDE DI ABBASSARE LE IMPOSTAZIONI DI SICUREZZA ALL'APERTURA.



# LA CULTURA DELLA CYBER SICUREZZA

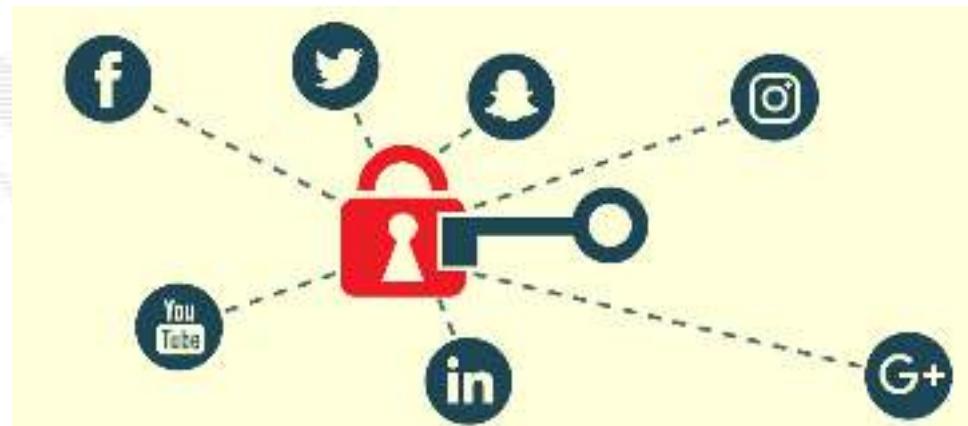
## PRESTARE ATTENZIONE ALL'USO DEI SOCIAL MEDIA

- I SOCIAL MEDIA RACCOLGONO E CONDIVIDONO DATI PERSONALI
- E' NECESSARIO ESSERE CONSAPEVOLI DELLE INFORMAZIONI CHE SI CONDIVIDONO ONLINE, SU SE STESSI E/O SULLA PROPRIA FAMIGLIA O ANCHE CON ALTRI NELLE COMUNICAZIONI/CONDIVISIONI TELEMATICHE
- I SITI DI SOCIAL NETWORK (FACEBOOK, INSTAGRAM, LINKEDIN ECC.) POSSONO ESSERE UTILIZZATI DAGLI AGGRESSORI PER RACCOGLIERE INFORMAZIONI ED UTILIZZARLE A PROPRIO VANTAGGIO
- CONTROLLARE SEMPRE LE PROPRIE IMPOSTAZIONI DI CONDIVISIONE PER LIMITARNE LA DIFFUSIONE CON UTENTI NON PIENAMENTE ATTENDIBILI

### SOCIAL PRIVACY COME TUTELARSI NELL'ERA DEI SOCIAL NETWORK



FONTE: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3140059>



FONTE: <https://www.e-legal.it/2016/05/15/marketing-a-prova-di-privacy-nel-social/>



# LA CULTURA DELLA CYBER SICUREZZA

## COME AVVENGONO GLI ATTACCHI INFORMATICI

### 1 INDIVIDUAZIONE DEL TARGET

Si identifica l'obiettivo da colpire e se ne studiano le mosse. Attraverso tecniche come il social engineering si raccolgono informazioni sul target e sul sistema di sicurezza.

### 2 INTRUSIONE

Grazie alle informazioni raccolte si cerca di ottenere il controllo del dispositivo da remoto. Attraverso tecniche quali il phishing, è possibile appropriarsi delle credenziali del network di protezione o tentare di installare un malware.

### 3 STUDIO DEL NETWORK

Nel corso di tentativi di mappare rete, porte di accesso e vulnerabilità, si individuano data base ed eventuali access point.

### 4 ACCESSO AI DATI

Con le credenziali di accesso ottenute, si prende il controllo dei sistemi informatici e dei relativi dati. Per mantenere l'accesso, si cercherà di installare strumenti come backdoors, rootkits o trojan.



*Grazie per l'attenzione*