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

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. E' NECESSARIO PRESTARE PARTICOLARE ATTENZIONE ALLA GESTIONE DEI COSIDDETTI DATI SENSIBILI PENA L'INCORRERE IN SANZIONI

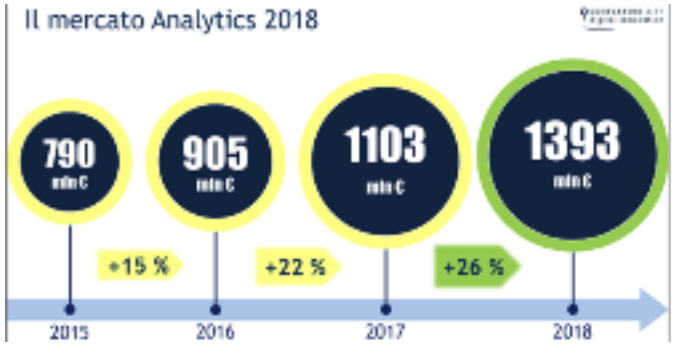
LINKED OPEN DATA

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

BIG DATA

FONTE: https://www.sadasdb.com/cosa-sono-big-data-quali-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 !!!

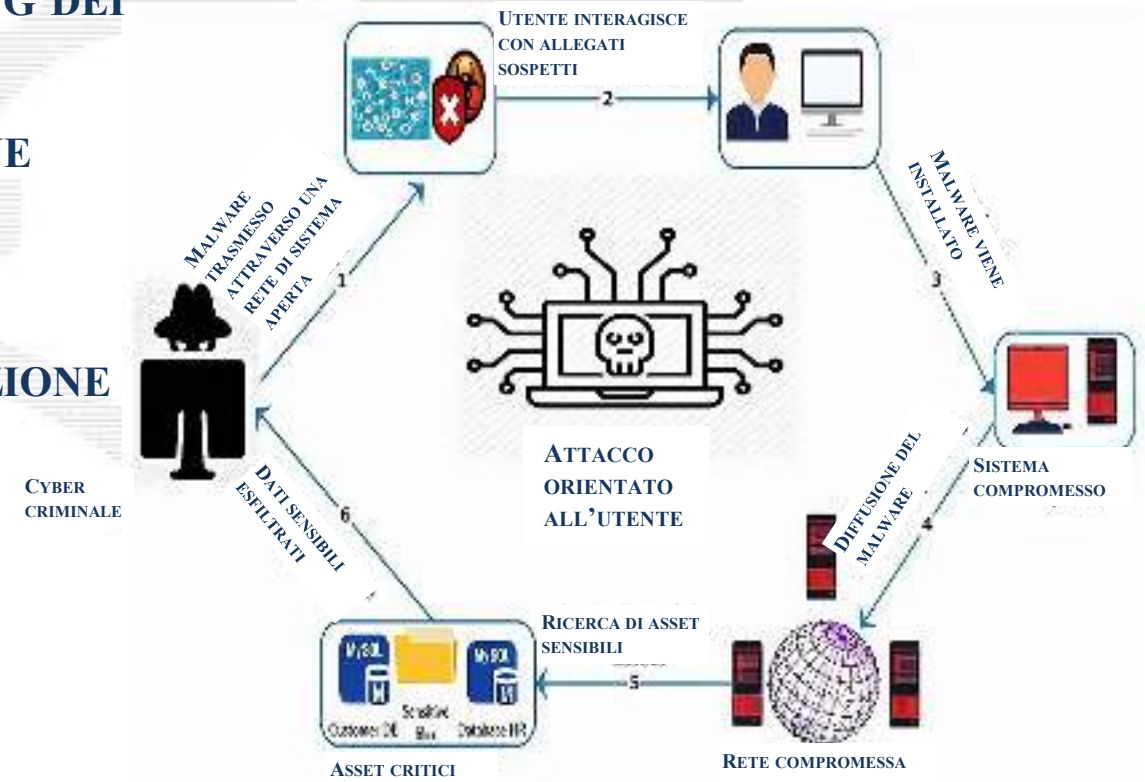
PERCHÉ IN REALTÀ …

- **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…

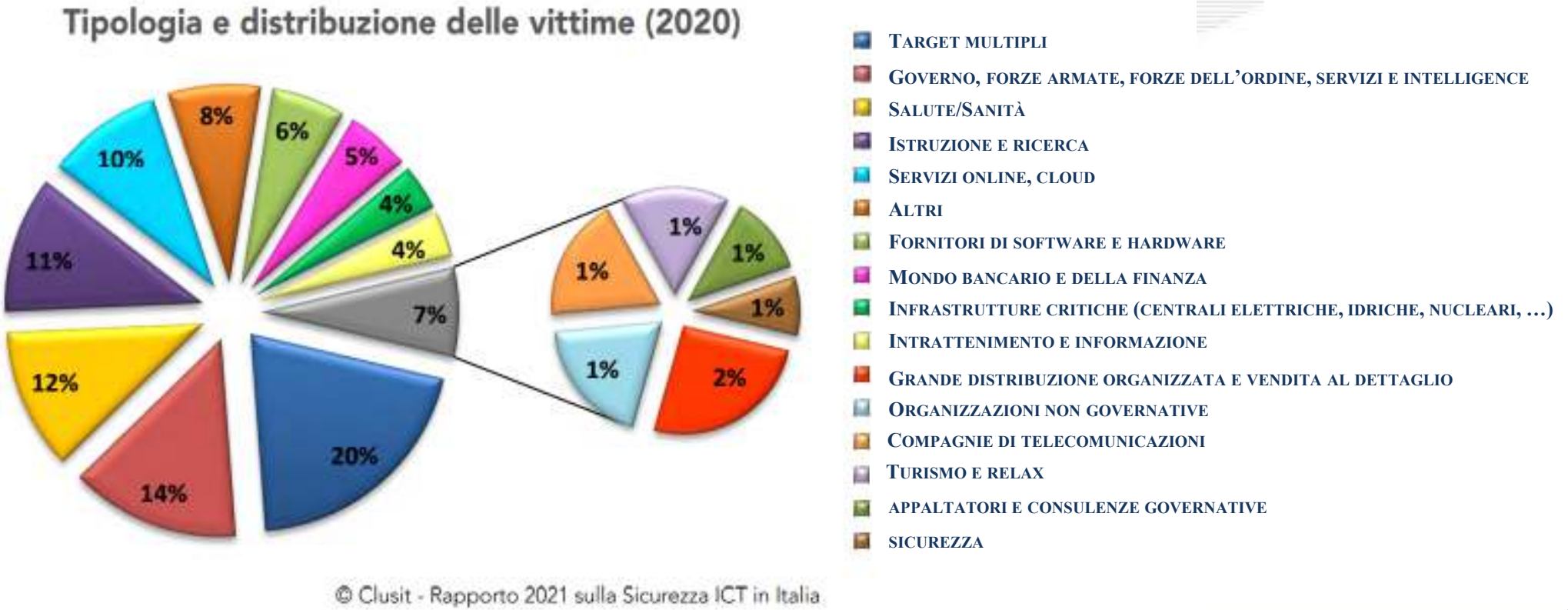


FONTE: https://www.frontiersin.org/articles/10.3389/fcomp.2020.00025/full

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

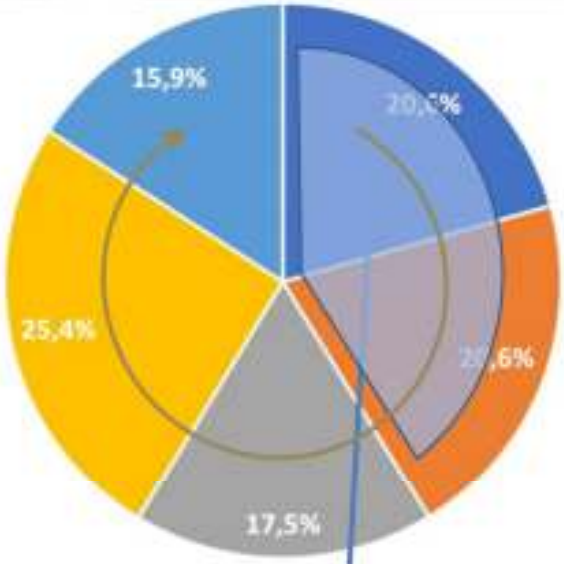


LA CULTURA DELLA CYBER SICUREZZA

ALCUNI DATI AL RIGUARDO …

ATTACCO INFORMATICO

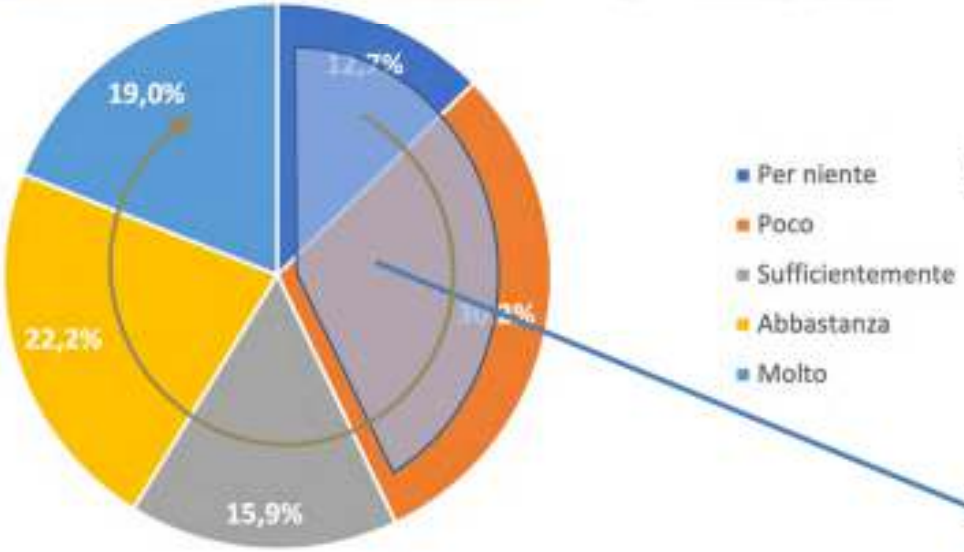
CAPACITÀ DI DIFESA



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.

CONSAPEVOLEZZA SUI RISCHI



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

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

FONTE: https://limeproxies.netlify.app/blog/top-10-information-security-threats-in-2018/

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 INFEZIONE TIPICI DEI RANSOMWARE SONO:

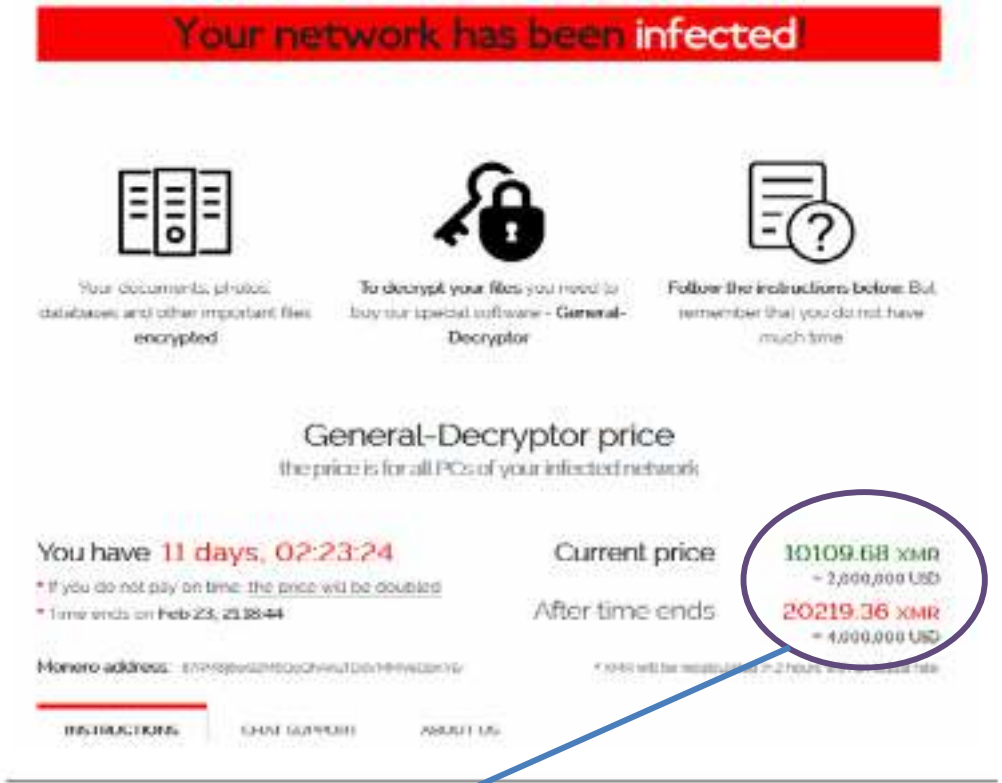
- INVIO DI EMAIL CONTENENTI ALLEGATI INFETTI O COLLEGAMENTI A SITI ESTERNI
- NAVIGAZIONE SU SITI COMPROMESSI
- VULNERABILITÀ DELLA RETE AZIENDALE

https://www.wired.it/internet/web/2021/07/10/cybersecurity-ransomware-sequestro-dati-cosa-sono/

LA CULTURA DELLA CYBER SICUREZZA

RANSOMWARE

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



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

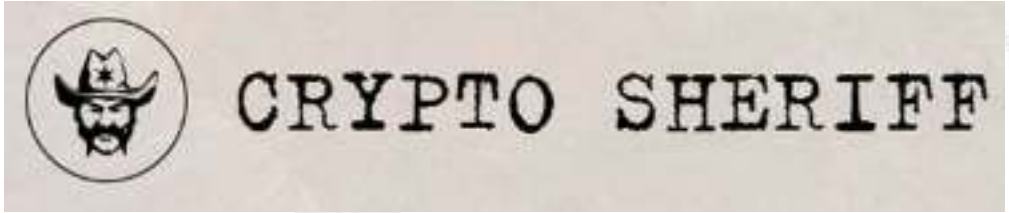
RISCATTO MOLTO SALATO

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 DECRIPTARE I DATI COLPITI DA DIVERSI TIPI DI RANSOMWARE (WWW.NOMORERANSOM.ORG)



FONTE: https://www.secplicity.org/2016/07/28/ransomeware-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

FONTE: https://www.insidemarketing.it/glossario/definizione/phishing/

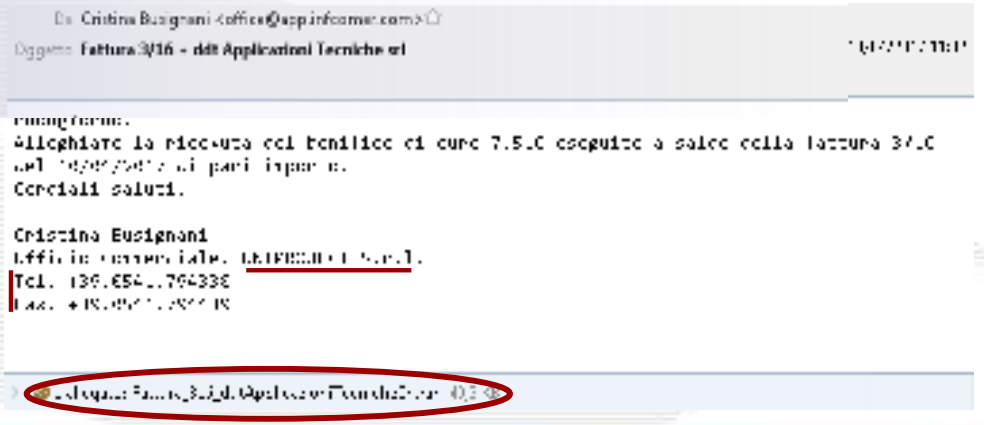
LA CULTURA DELLA CYBER SICUREZZA

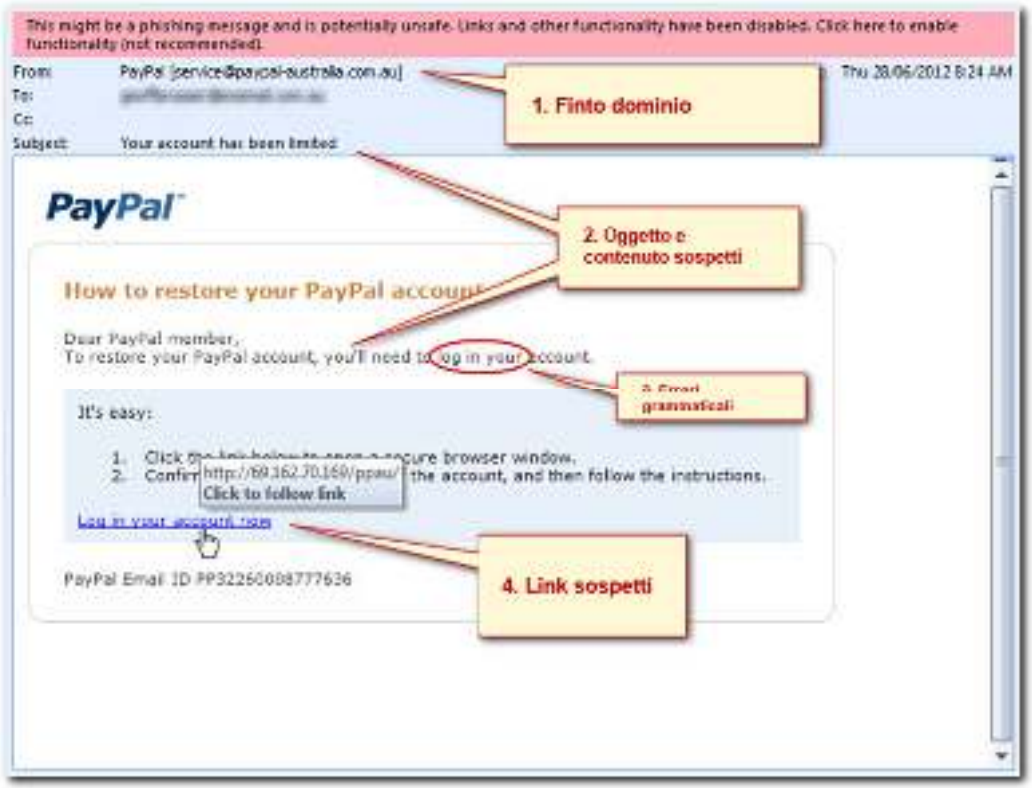
PHISHING

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

LA CULTURA DELLA CYBER SICUREZZA

PHISHING





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
- SPESSO SONO CONTENUTI IN ALLEGATI IN FORMATO WORD, EXCEL O PDF CHE DEVONO ESSERE APERTI PRIMA CHE IL MALWARE SI ATTIVI.
- SPESSO I MALWARE TRAGGONO VANTAGGIO DAI SOFTWARE O SISTEMI OPERATIVI NON AGGIORNATI
- ALCUNI MALWARE RICHIEDONO L'ABILITAZIONE DELLE MACRO: SOSPETTARE SEMPRE DI UN ALLEGATO CHE RICHIEDE 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

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


Grazie per l'attenzione