Alcuni consigli su come proteggersi dai malware

Non serve essere tecnici informatici

- Non siamo tutti tecnici informatici ma è necessario avere conoscenze informatiche di base che ci consentano di utilizzare i dispositivi tecnologici e di navigare in Internet mantenendo nella massima sicurezza possibile i nostri dati ed eventualmente quelli della rete a cui i nostri dispositivi sono collegati.
- Bisogna essere consapevoli che le informazioni personali degli utenti che trattiamo quotidianamente ci sono state affidate e devono essere custodite nella massima sicurezza possibile.

Malware

- Con il termine **malware** (dalla contrazione delle due parole inglesi “malicious” e “software”, letteralmente “programma maligno” o “codice maligno”) si indica genericamente un qualsiasi software, ovvero un qualsiasi programma, creato con lo scopo di causare danni più o meno gravi ad un computer o a un qualsiasi sistema informatico su cui viene eseguito ed ai dati degli utenti in esso contenuti. All’interno della categoria dei malware esistono una serie di programmi ognuno dei quali agisce con modalità differenti e con obiettivi specifici particolari.
- Virus, **worm** (“vermi” informatici) o **trojan** (“cavalli di Troia”) nonché **spyware**, possono causare la perdita di dati con gravi pregiudizi alla sfera privata.
- **Hoax** o **spam** sono spesso solo fastidiosi, qualora si adottino le appropriate contromisure comportamentali
- La tecnica del **phishing** può portare alla perdita di informazioni personali estremamente delicate.

Virus

- Un virus è un programma informatico composto da un numero molto ridotto di istruzioni elementari, specializzato per eseguire soltanto poche e semplici operazioni ed ottimizzato per impiegare il minor numero di risorse, in modo da rendersi il più possibile invisibile.
- Caratteristica principale di un virus è quella di riprodursi e quindi diffondersi nel computer ogni volta che viene aperto un file infetto.
- Lo scopo dei virus è quello di creare danni, fastidi e disagi a chi lo riceve, non ultimo quello della perdita totale dei dati o il furto di importanti informazioni.

Come avviene l'infezione

- L'infezione da virus avviene mediante l'esecuzione di un file contenente, in modo diretto o indiretto, il codice virale.
- Il virus si può trasmettere mediante un accesso fisico al PC, con l'utilizzo di un supporto di memorizzazione (CD o unità **USB)** da parte dell'utente malevolo o, inconsapevolmente, della vittima stessa.
- Ma il malware può anche essere **allegato a messaggi di posta elettronica** (**spam**): l'utente viene così invitato ad aprire l'allegato, che può essere un file eseguibile o anche un documento elettronico.
- Infine l'introduzione del virus può avvenire anche via Web (e ad oggi questo è il canale di diffusione più frequente) trasmettendo il codice malevolo attraverso un **download da una pagina Web**.

Worm (Vermi)

- Come i virus, i **worm** (dall'inglese: "vermi") sono dei programmi opportunamente progettati per danneggiare l'utente, ma, contrariamente ai virus, non necessitano di un programma ospite per funzionare, essendo essi stessi dei programmi completi.
- Essi sfruttano lacune di sicurezza (in gergo "vulnerabilità") o errori di configurazione del sistema operativo per propagarsi autonomamente da un computer all'altro, tipicamente attraverso Internet.

Trojan (Cavalli di Troia)

- I **trojan** (letteralmente "cavalli di Troia") sono programmi che eseguono di nascosto operazioni nocive, celandosi all'interno di applicazioni e documenti utili per l'utente.
- I trojan sfruttano lacune di sicurezza dei programmi utilizzati per aprire i file infetti e installarsi nel sistema ad insaputa dell'utente. Per esempio, **potrebbero trovarsi all'interno di brani musicali .mp3** e sfruttare una qualche vulnerabilità del programma di riproduzione, soprattutto qualora questo non fosse aggiornato all'ultima versione.
- Spesso i trojan **sono programmi scaricati da internet**, altre volte vengono propagati per il tramite di **allegati alle email**.

Spyware e Grayware

- Con i termini **spyware** e **grayware** si definiscono le applicazioni o i file non classificati come virus o cavalli di Troia, che tuttavia hanno un effetto negativo sulle prestazioni dei computer.
- Spyware e grayware introducono notevoli rischi per la sicurezza, la riservatezza e conformità legale nelle organizzazioni. Spesso spyware e grayware attivano una varietà di azioni indesiderate e pericolose, come la visualizzazione di fastidiose finestre pop-up, la registrazione delle sequenze di tasti premute dall'utente o l'esposizione delle vulnerabilità del computer agli attacchi.
- Lo "**spyware**" (termine derivante dalla contrazione delle parole inglesi "*spy*" e "soft*ware*") è destinato a raccogliere informazioni all'insaputa dell'utente per trasmetterle a un indirizzo predefinito. Il tipo di informazioni lette varia da uno spyware all'altro e può riguardare le abitudini di navigazione dell'utente, le configurazioni di sistema e persino le password.

Grayware e Adware

- Il termine di "**adware**" deriva dalla contrazione delle parole inglesi "*ad*vertising" (pubblicità) e "soft*ware*". In genere l'adware è utilizzato a scopi pubblicitari, nel senso che le abitudini di navigazione dell'utente vengono registrate e sfruttate per offrirgli prodotti corrispondenti (ad es. per il tramite di link personalizzati), pur senza che questi ne abbia fatto richiesta esplicita.
- **Spyware, Grayware, Adware si installano solitamente sul computer quando si scaricano programmi.** La maggior parte dei programmi contiene un contratto di licenza per l'utente finale che l'utente deve accettare prima di avviare il download. Spesso nel contratto di licenza viene spiegato che l'applicazione effettuerà una raccolta di dati personali, tuttavia molto frequentemente, gli utenti non leggono attentamente il contratto e così non si limitano a scaricare il programma di cui avevano bisogno.

Phishing

- La parola phishing deriva dalla contrazione delle parole inglesi "password", "harvesting" (raccolta) e "fishing" (pesca).
- Il *phishing* è un **tentativo di truffa**, realizzato solitamente sfruttando la posta elettronica, che ha per scopo il furto di informazioni e dati personali degli utenti. I mittenti delle **email di** *phishing* sono (o meglio, sembrano essere) organizzazioni conosciute, come banche o portali di servizi web, e hanno apparentemente uno scopo informativo: avvisano di problemi riscontrati con account personali dell'utente (*home banking*, portali di aste online, provider di posta elettronica, social network e altro) e forniscono suggerimenti su come risolvere le problematiche. Nella stragrande maggioranza dei casi, sarà suggerito di cliccare su qualche link e fornire informazioni e dati personali per ripristinare l'account o metterlo al sicuro. **Nel caso in cui si cliccasse sul collegamento e si fornissero le informazioni richieste, si finirebbe diritti nella *rete* dell'*hacker*-pescatore.**

Hoax (Bufale)

- Le email contenenti informazioni su nuovi virus o presunti tali sono quasi sempre notizie false ("**hoax**", termine inglese per designare scherzi o notizie false). In genere si viene messi in guardia contro nuovi virus estremamente pericolosi, impossibili da combattere anche con i normali antivirus e si viene invitati a diffondere la notizia a tutti i conoscenti o a seguire delle istruzioni per evitare la minaccia. Possiamo definirle "catene di sant'Antonio digitali", il cui obiettivo è quello di far circolare il messaggio con un contenuto spesso assurdo e che fa generalmente leva su aspetti scaramantici o emotivi, causando perdite di tempo e spreco di banda.

Spam

- Con "**spam**" si indicano generalmente tutte le email indesiderate, con un contenuto di vario genere, da quello pubblicitario, a quello più o meno fantasioso ed assurdo, tipico delle catene di sant'Antonio.
- Lo "spammer" è il mittente di queste comunicazioni, mentre il fenomeno del loro invio è denominato "spamming".
- Lo spammig porta ad una notevole perdita di tempo da parte di chi riceve il messaggio, anche semplicemente per la sua cancellazione.

Gli attacchi cyber in Italia e nel mondo

- Secondo i dati del Rapporto Clusit 2017, presentati al Cyber Security 360 Summit, sono 571 a livello globale gli attacchi di dominio pubblico avvenuti da gennaio a giugno 2017, con un impatto significativo per le vittime, in termini di danno economico, reputazione e diffusione di dati sensibili: il peggiore semestre di sempre, con una crescita costante dal 2011 ad oggi.
- Oltre il 50% delle organizzazioni nel mondo ha subito almeno un'offensiva grave nell'ultimo anno. La maggior parte degli attacchi (il 36%) è stata sferrata con malware (+86% rispetto al secondo semestre 2016), ma crescono (+85%) anche gli attacchi via Phishing e Social Engineering (manipolazione psicologica delle persone che le induce a compiere determinate azioni o a divulgare informazioni riservate).

CYBER SECURITY 360 Summit

Il pericolo oggi si chiama Ransomware

- **Ransomware:** è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (*ransom* in inglese) da pagare per rimuovere la limitazione.
- Questa famiglia di malware – non esiste un solo tipo di virus del riscatto, infatti – è in grado di bloccare il funzionamento del computer, facendo sì che l'utente non riesca a effettuare il login nel suo profilo utente (mostrando, solitamente, un avviso dell'FBI o della Polizia di Stato) o utilizzando la crittografia per rendere illeggibili i file presenti all'interno del disco rigido (questi ransomware sono chiamati **cryptolocker**, dal momento che utilizzano la crittografia per bloccare i file). WannaCry, tanto per fare un esempio, appartiene proprio a questa seconda categoria.

I ransomware preferiscono le email

- Al primo posto, tra le tipologie di malware trasmesse per email, si trovano i *ransomware*. Secondo l'azienda di cybersecurity Proofpoint, il virus del riscatto è stato trovato nel 68% dei messaggi di posta elettronica contenenti una qualsiasi forma di programma malevolo.

I punti deboli sfruttati da Malware e Ransomware

- **Vulnerabilità software dei sistemi**: aspetti del sistema per i quali le misure di sicurezza non sono adeguate o sono compromesse e di conseguenza più facilmente attaccabili.
- **Formazione degli utenti**: *Virus e truffe online* Il 74% degli utenti non ha le competenze necessarie per riconoscere i pericoli online. A rivelarlo è un test realizzato da Kaspersky Lab sulle abitudini di 18.000 utenti.
- **Comportamenti non appropriati** degli utenti: ad esempio apertura di allegati sospetti per disattenzione e/o curiosità.

Come difendersi

- Leggere sempre con attenzione i messaggi visualizzati nel PC e in particolare durante la navigazione, prima di cliccare su SI.
- È fondamentale ai fini della sicurezza scaricare gli **aggiornamenti del software** (software update, chiamate anche“patch”), perché consentono di colmare le falle di sicurezza che vengono scoperte quasi quotidianamente, le cosidette vulnerabilità del Sistema; è consigliabile programmare gli aggiornamenti in automatico.
- In caso di problemi o difficoltà, è consigliabile rivolgersi a ditte specializzate.

Verificare l'installazione del programma antivirus e tenerlo aggiornato

- Un software antivirus aggiornato è assolutamente **indispensabile**. Dato che giornalmente nascono numerosi nuovi malware, è tassativamente indispensabile anche un **aggiornamento frequente** del software antivirus.
- La maggior parte dei prodotti dispongono di funzioni automatiche di aggiornamento che devono essere assolutamente attivate.

Cosa non fare

- **NON aprire chiavette USB** sulla propria postazione di lavoro, magari per caricare il file di un collega.
- **NON scaricare programmi da internet** se non con l'assistenza di una persona esperta e solo dopo aver verificato l'attivazione dell'antivirus e il suo aggiornamento; accertarsi di essere sul sito del produttore del software.
- **NON scaricare programmi sconosciuti.**
- **NON scaricare** musica, film, file con estensioni: zip, exe, bat, dll o non conosciute.
- **NON navigare sui social** e/o su siti non conosciuti.

Attenzione alle email

- Usare **prudenza nella apertura di email con mittente ignoto**;
- **diffidare delle email di cui non si conosce l'indirizzo del mittente**; in questo caso non aprire mai gli allegati o i programmi ivi contenuti, né selezionare i link indicati;
- aprire unicamente i file o i programmi provenienti da **fonti affidabili** e solo previa verifica con un programma antivirus aggiornato;
- **diffidare dei file con due estensioni:** non aprire mai gli allegati di email provvisti di due estensioni (ad es. picture.bmp.vbs o pdf.exe) e non lasciarsi ingannare dall'icona di simili file; disattivare nelle opzioni del browser, dove presente, l'opzione "nascondi le estensioni per i tipi di file conosciuti; i file firmati possono presentare due estensioni, ad es. .pdf.p7m, accertarsi comunque della fonte prima di aprirli.

Attenzione alle email

- **Non rispondere alle spam:** rispondere ad un messaggio di spam equivale ad informare lo spammer che l'indirizzo email è valido e quindi questi invierà ulteriori spam oppure metterà il vostro indirizzo a disposizione di altri spammer; particolare attenzione va portata agli spam con l'opzione di "cancellazione dall'elenco" in cui si promette la cancellazione dall'elenco di distribuzione tramite l'invio di un'email con un determinato contenuto.
- **controllare l'indirizzo del mittente:** passare sempre il mouse sopra l'indirizzo: apparirà un collegamento ipertestuale; è importante che il link visualizzato dopo il passaggio con il mouse resti identico, altrimenti molto probabilmente si tratta di un tentativo di truffa con un indirizzo fasullo.

Attenzione alle email

- **Verificare sempre la validità di un indirizzo o di un link** ricevuto via e-mail: a volte gli indirizzi cambiano di poco (anche per una sola una vocale o consonante diversa); altre volte vengono aggiunte delle parti all'apparenza non dubbie, ma che poi rimandano a siti ingannevoli.
- Prestare **attenzione alla grammatica e all'ortografia**: spesso chi crea una campagna di *phishing* non proviene dall'Italia; è probabile che il messaggio ricevuto presenti una URL all'apparenza valida e anche il nome del mittente ricordi quello della nostra banca, di un'azienda o di un amico ma se il testo presenta errori nei tempi verbali, negli accenti, o nella costruzione della frase , è molto probabile che si tratti di una truffa, questo perché il testo è stato quasi certamente tradotto da un'altra lingua.

Attenzione alle email

- **Diffidare delle email** scritte **in inglese** provenienti da mittenti sconosciuti.
- **Diffidare delle offerte irrifiutabili:** quando una cosa sembra troppo bella per essere vera, molto probabilmente non è vera. Se riceviamo un messaggio da un utente sconosciuto che ci promette a prezzi stracciati smartphone, tablet o accessori hi-tech, vincite alla lotteria …. si tratta di una truffa.
- **Diffidare** anche **delle email di offerte** che assomigliano a quelle che si ricevono solitamente da siti e-commerce.

Attenzione alle email

- **Diffidare di email apparentemente provenienti da enti governativi o pubblici**: i cyber criminali a volte fingono di essere un'istituzione; è bene ricordare, che i vari enti non utilizzano la posta elettronica per certi tipi di comunicazioni; ad esempio, è improbabile che il Comune o altre istituzioni ci scrivano via email per chiederci dei soldi o informazioni riservate e che l'Agenzia delle Entrate mandi alla scuola un accertamento fiscale via email.
- **Non aprire mai allegati tipo fattura elettronica**: la scuola riceve solo fatture elettroniche via SIDI; se si consce il fornitore contattarlo al telefono.

Come intervenire

- La sicurezza dei dati personali degli utenti **dipende principalmente dall'attenzione** degli operatori.
- In caso di infezione **spegnere il PC, staccarlo dalla rete,** se connesso via cavo, rivolgersi al personale tecnico della scuola o chiamare l'assistenza**.**