Alcuni consigli su come proteggersi dai malware

Non serve essere tecnici informatici

- Non tutti siamo tecnici informatici: giusto.
- Però ad esempio: quando vogliamo prendere la patente di guida, pur non essendo tutti meccanici o elettrauto, ci vengono chieste anche conoscenze di base sul funzionamento del motore, degli «strumenti di bordo» necessari a condurre in **sicurezza** l'autoveicolo.
- Lo stesso accade, quando siamo chiamati a «guidare» il nostro PC, non siamo tecnici informatici, ma è necessario avere conoscenze informatiche di base che ci consentano di usarlo e «navigare» tenendo nella massima sicurezza possibile i nostri dati e quelli della nostra rete. Bisogna essere consapevoli che le informazioni personali degli utenti che trattiamo quotidianamente non sono nostre, 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
- il virus è, propriamente, un ben preciso tipo di malware): 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.

I 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. Ovviamente 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.

- Come avviene solitamente l'infezione: l'introduzione avviene mediante l'esecuzione di un file contenente, in modo diretto o indiretto, il codice virale. Tale introduzione che può avvenire mediante il trasferimento fisico, modalità, molto diffusa in passato, ma ancora oggi frequente, prevede l'uso di un supporto di memorizzazione (CD o unità **USB)** da parte dell'utente malevolo o, inconsapevolmente, della vittima stessa e prevede un accesso fisico al PC.
- 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 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**.

I 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 invece lacune di sicurezza (in gergo "vulnerabilità") o errori di configurazione del sistema operativo per propagarsi autonomamente da un computer all'altro. Obiettivo dei worm sono computer che presentano lacune di sicurezza o errori di configurazione e che sono collegati ad altri computer, tipicamente attraverso internet.

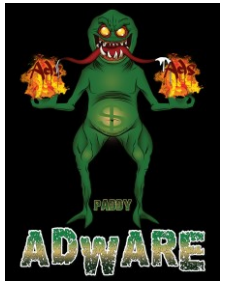
Trojan (Cavalli di Troia)

- I **trojan** (letteralmente “cavalli di Troia”) sono programmi che eseguono di nascosto operazioni nocive, nascondendosi all’interno di applicazioni e documenti utili per l'utente. Questi sfruttano lacune di sicurezza dei programmi utilizzati per aprire i file infetti per 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**.

Grayware e Spyware

- 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 della rete. 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 all'insaputa dell'utente informazioni sulle sue abitudini di navigazione oppure sulle configurazioni di sistema per trasmetterle a un indirizzo predefinito. Il tipo di informazioni lette varia da uno spyware all'altro e può spaziare dalle abitudini di navigazione sino alle 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.

IL 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", l'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, 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 per la sua sola cancellazione.

Gli attacchi cyber in Italia e nel mondo

Secondo i dati del Rapporto Clusit 2017 presentati al Cyber Security 360 Summit, infatti, 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 anche gli attacchi via Phishing e Social Engineering (+85%).

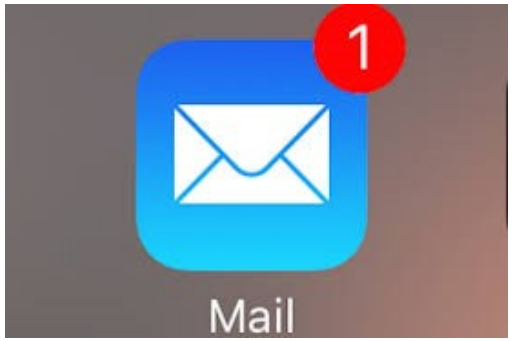
CYBER SECURITY 360 Summit

Il pericolo oggi si chiama: Ransomware

Ransomware: la traduzione letterale dall'inglese è "virus del riscatto", definizione che in qualche modo ci aiuta già a capirne il funzionamento. 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 e-mail

- 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**: affidarsi ad aziende, professionisti, esperti in grado di tenere aggiornate le vulnerabilità delle dotazioni informatiche della scuola.
- **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.

COSA FARE ?

- Particolarmente importanti ai fini della sicurezza sono 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.
- Questi aggiornamenti, meglio siano automatici, richiedere di programmarli al personale tecnico che cura l’assistenza informatica della vostra struttura.

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** senza 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

- *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**
- *verifica dell'affidabilità della fonte:* aprire unicamente i file o i programmi provenienti da fonti affidabili e solo previa verifica con un programma antivirus aggiornato
- *attenzione ai file con due estensioni:* non aprire mai gli allegati ad 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 della fonte prima di aprirli.

- *non rispondere agli 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'URL*: una delle primissime cose da fare per verificare la validità di un'e-mail è quella di guardare la URL. Alle volte un testo scritto bene e valido all'apparenza presenta una URL fasulla. Altre volte l'URL sembra combaciare perfettamente con il testo e le richieste scritte nella conversazione. Per essere sicuri però passiamo sempre il mouse sopra l'indirizzo. In questo caso apparirà il collegamento ipertestuale. È importante che anche nel link visualizzato dopo il passaggio con il mouse resti identico. Altrimenti state certi che si tratta di un tentativo di truffa con una URL fasulla.

- *URL con dominio ingannevole*: la fretta è cattiva consigliera. Sempre, soprattutto quando stiamo verificando la validità di un indirizzo o di un link ricevuto via e-mail. Bisogna prestare molta attenzione perché alle volte gli indirizzi cambiano di poco. Alle volte è una vocale o una consonante ad essere diversa e altre volte vengono aggiunte delle parti all'apparenza non dubbie, ma che poi rimandano a siti ingannevoli. Pensiamo al prefisso Info e così via davanti al normale dominio del mittente dal quale di solito riceviamo posta non ingannevole
- *Attenzione alla grammatica*: spesso e volentieri chi crea una campagna di phishing non proviene dall'Italia. Uno degli aspetti da tenere più in considerazione dunque è la grammatica, così come l'ortografia. È probabile che il messaggio ricevuto presenti una URL all'apparenza valida e anche il nome del mittente ricordi quello della nostra banca, dell'azienda di lavoro o di un amico. Se il testo presenta diversi errori nei tempi verbali, negli accenti o nella costruzione della frase però è molto probabile che si tratti di una truffa. Questo perché il testo è stato quasi certamente tradotto da un'altra lingua.

- *Le 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 …. state pur certi che si tratta di una truffa. E fate attenzione anche alle email di offerte che si assomigliano a quelle che ricevete solitamente da siti e-commerce.
- *Gli enti governativi*: c'è un mittente al quale, tutti o quasi, diamo credito. Gli enti governativi e le istituzioni. È difficile pensare che uno di questi ci voglia truffare via e-mail. I cyber criminali lo sanno, e per questo motivo alle volte fingono di essere un'istituzione. Bisogna ricordare, però, che i vari enti non utilizzano la posta elettronica per un certo tipo di comunicazione e comunque bisogna prestare sempre attenzione. È impossibile che il Comune o altre istituzioni ci scrivano via e-mail per chiederci dei soldi o delle informazioni molto riservate. Improbabile che l'Agenzia delle Entrate mandi alla scuola un accertamento fiscale via email.

- *Attenzione alle email scritte in inglese*
- *Non aprire mai allegati tipo*: fattura elettronica, la scuola riceve solo fatture elettroniche via SIDI. Se si consce il fornitore contattarlo al telefono.
- Leggere sempre con attenzione i messaggi visualizzati nel PC e in particolare durante la navigazione, prima di cliccare su SI.

La sicurezza dei dati personali affidateci dagli utenti, **dipende principalmente dall'attenzione** che mettiamo nella «guida e navigazione» del nostro PC.

Cosa fare in caso di infezione?

Spegnere il PC, staccarlo dalla rete e chiamare l'assistenza.

Seguire le istruzioni previste nei casi di infezione da virus dal piano della sicurezza informatica della scuola.