White Paper

Phishing: cos’è e come evitarlo

NON CI SONO PIÙ GLI HACKER DI UNA VOLTA

Difficile che trascorra qualche giorno senza che i media non riportino notizia di qualche azienda, ente pubblico o organizzazione a cui dei cybercriminali abbiano razziato informazioni, sottratto denaro o bloccato i computer chiedendo un riscatto.

Sono notizie che tutti leggiamo con una punta di divertimento **pensando che tanto no, *a noi non può succedere*.**

In fondo manteniamo i nostri sistemi operativi sempre aggiornati, siamo dotati dei più moderni software di sicurezza e antivirus, la nostra rete è protetta da sofisticati firewall e i nostri consulenti IT vigilano costantemente affinché tutto funzioni regolarmente. Non possiamo nemmeno accedere alla rete aziendale dai nostri smartphone personali né navigare su siti discutibili: *quindi* **dobbiamo proprio essere in una botte di ferro.**

Oppure no?

C'è una cosa che i media si dimenticano sempre di dire quando raccontano di campagne di attacchi e truffe informatiche andate a buon fine: che fino a quel momento anche le vittime avevano vissuto con la medesima sensazione di sicurezza, per le medesime buone ragioni. Approfondisci le casistiche, e scoprirai che le aziende colpite non mancavano certo né di firewall, né di software per la sicurezza, né di specialisti IT capaci.

Ma allora **perché i cybercriminali riescono a colpire con successo in modo così frequente?**

Semplicemente perché hanno lasciato perdere gli attacchi puramente tecnici – computer contro computer, per intenderci – **concentrandosi invece sul vero anello debole della catena: l'essere umano.**

E per questo sfruttano un canale di contatto diretto che, per propria natura, si presta bene ad aggirare le difese tecnologiche arrivando a colpire il fianco scoperto degli spesso distratti utenti: **la posta elettronica**.

Questo sistema di attacco **si chiama *phishing***, e nelle pagine che seguono impareremo a conoscerlo, affrontarlo e, soprattutto, a neutralizzarlo.

PESCA PESCA, PRIMA O POI ABBOCCANO: IL PHISHING

Alzi la mano chi non ha mai ricevuto un messaggio email, scritto a nome di qualche istituto bancario, servizio di pagamento, sito e-commerce, corriere, utility, operatore Internet o altro brand conosciuto che invita, magari in un italiano stentato e zeppo di errori ortografici, a confermare le proprie credenziali utente attraverso un link appositamente fornito, a scaricare una presunta fattura o a leggere attentamente le importanti informazioni contenute in un documento allegato.

Messaggi di questo genere spediti automaticamente a milioni di indirizzi attraverso vere e proprie campagne di spam hanno dato vita alla **prima generazione di attacchi di *phishing*** – storpiatura dell'inglese *fishing*, pescare – il cui impatto è risultato certamente fastidioso ma non più di quel tanto pericoloso. I maldestri tentativi di impersonare persone od organizzazioni conosciute e di fiducia si sono inizialmente arenati contro un'esecuzione a dir poco approssimativa e dalla natura truffaldina facilmente identificabile.

Ma, come era immaginabile, è stato sufficiente solo poco tempo affinché i delinquenti da tastiera imparassero la lezione **rendendo più credibili le loro richieste**.

In fondo la cosa veramente importante si trova nell'idea di fondo di questi attacchi: **spacciarsi per un mittente noto così da far abbassare il normale livello di cautela** che tutti esercitiamo quando riceviamo messaggi non richiesti da perfetti sconosciuti, spingendo quindi l'inconsapevole utente a compiere un'azione capace di mettere in moto il meccanismo della truffa senza che ciò risulti evidente. Le due casistiche più comuni sono le seguenti:

- **con la scusa di un account bloccato**, viene chiesto all'utente di **verificare i propri dati personali** su un sito controllato dal truffatore. Il messaggio email contiene un link che rimanda a **una pagina web dall'aspetto simile a quello del sito ufficiale** del preteso mittente, dove l'utente deve compilare un modulo con le informazioni richieste: username, password, data di nascita, codice fiscale e tutto quello che il cybercriminale intende carpire alla sua vittima. **L'utente poco accorto rivela in questo modo le credenziali** che potranno essere utilizzate per accedere ai sistemi dell'organizzazione di cui si sono prese le sembianze, nonché altre informazioni riservate che potranno essere rivendute con profitto nel cosiddetto dark web;
- **fare in modo che l'utente apra un file contenente malware**. Questo avviene **simulando l'invio di una fattura**, di un estratto conto, di una bolletta di spedizione o di una comunicazione ufficiale che in realtà nasconde al proprio interno software pericoloso o sfrutta vulnerabilità note di diffusi formati come quelli dei **documenti Office o PDF**. In genere è il veicolo prediletto per diffondere il **ransomware**, ovvero quel particolare tipo di malware che rende inaccessibili i file di un computer cifrandoli crittograficamente e invitando la vittima a pagare un riscatto per ottenere la chiave di decifrazione, ma è perfetto anche per installare spyware o assumere il controllo della macchina colpita sfruttandola a scopi illegali come invio di spam, mining di criptovalute o attacchi DDoS contro terzi.

In tutti questi casi le email hanno **un aspetto simile o identico a quello dei messaggi inviati normalmente dall'organizzazione legittima**, e nei casi più sofisticati i link eventualmente presenti rimandano a domini dal nome pressoché uguale, magari approfittando di similitudini tipografiche tra lettere differenti: è sufficiente sostituire una L minuscola con una I maiuscola o scegliere un dominio geografico simile (come .lt, Lituania, al posto di .it). Il testo è scritto correttamente in buon italiano seguendo esattamente lo stile grafico e formale delle comunicazioni del legittimo mittente, tanto che **diviene sempre difficile capire quando ci si trova davanti a una mail fasulla**.

Anche i sistemi di sicurezza informatica come **antivirus e antispam faticano a bloccare questo tipo di minaccia** che, non a caso, è appositamente studiata per aggirare i meccanismi di rilevamento basati su elenchi di domini o presenza di file eseguibili. I link dannosi vengono infatti costantemente modificati, quindi gli aggiornamenti delle blacklist dei domini pericolosi non riescono a tenere il ritmo con cui i cybercriminali ne registrano di nuovi. E per quanto riguarda il malware, anche l'antivirus più efficace può fallire di fronte a codice criptato nascosto (o fatto scaricare volta per volta) all'interno di un documento Office a sua volta compresso come archivio ZIP.

Non ci è voluto molto perché le menti responsabili di questo genere di attacchi si rendessero conto che il meccanismo del phishing poteva essere messo meglio a frutto **personalizzandolo a livello individuale sulle potenziali vittime**.

Ecco dunque che ai tradizionali invii automatizzati di massa verso enormi quantità di indirizzi email si è presto aggiunto un modo più subdolo per colpire.

A PESCA CON L'ARPIONE: LO SPEAR PHISHING

Se la tradizionale pesca a strascico si basa in fondo sulla probabilità statistica di catturare qualche pesce che resti impigliato durante il passaggio delle reti, la pesca all'arpione è invece una faccenda completamente diversa che inizia selezionando accuratamente la preda desiderata per poi provare a colpirla.

La stessa differenza separa il normale phishing dal **cosiddetto *spear phishing***, termine che per l'appunto **richiama la pesca all'arpione** ("spear") dal momento che il cybercriminale agisce dopo aver scelto con attenzione l'obiettivo, averne studiato le caratteristiche e predisposto **comunicazioni su misura**. Si tratta di un'applicazione customizzata delle tecniche tipiche del phishing, ed è proprio la sua **personalizzazione a renderla ancora più letale** aumentandone l'efficacia.

Il lavoro di preparazione può essere più o meno impegnativo a seconda del target e del risultato che si intende ottenere, ma non è certo impossibile considerando la facilità con la quale è possibile oggi acquisire informazioni di ogni genere su chiunque.

Non sono solamente i **profili dei social media** (sia i nostri personali che quelli dei nostri conoscenti) a raccontare molto di noi – la nostra posizione lavorativa, i nostri interessi, la nostra rete di amicizie e di contatti – dal momento che vi sono **innumerevoli altre fonti** magari meno evidenti ma pur sempre efficaci: un'intervista, una presentazione a una conferenza, il video di un intervento a un evento aziendale, qualche commento in un forum di settore, e questo solo per restare nel contesto professionale.

Aggiungiamo quindi tutte le informazioni che vengono disseminate nell'ambito delle attività personali: sport, hobby, volontariato, partecipazione alla vita della propria comunità e così via.

Il cybercriminale ha quindi a disposizione un **enorme patrimonio di informazioni pubbliche** da sfruttare per risultare il più convincente possibile nel momento in cui aggancia la propria vittima **spacciandosi per una persona conosciuta**, magari un collega.

Il primo passo può essere un **semplice messaggio che ha lo scopo di avviare una conversazione**: nessun link strano, nessun allegato, nulla di sospetto, solo un modo per neutralizzare qualsiasi diffidenza e stabilire il rapporto.

Solo in un secondo momento arriverà la richiesta che di fatto attiva la truffa: fornire credenziali o dati sensibili, scaricare documenti che in realtà contengono malware, effettuare un'operazione di qualche tipo.

Un esempio pratico: uno spear phisher che voglia entrare all'interno della rete di un'azienda può iniziare a risalire all'organigramma dei dipendenti consultando LinkedIn.

Identificate le persone che ricoprono i ruoli più adatti rispetto all'obiettivo desiderato e le rispettive relazioni nell'ambito lavorativo, i motori di ricerca e i social media permettono di farsi un quadro più dettagliato di ciascun individuo e di avviare un vero e proprio stalking digitale.

Non appena un profilo Facebook o Instagram indicherà che uno dei dipendenti tenuti sotto controllo è partito per una vacanza in qualche destinazione lontana, sarà davvero un gioco da ragazzi inviare una mail amichevole a suo nome allegando documenti che la persona in questione avrebbe "dimenticato" di lasciare ai colleghi prima di andarsene in ferie.

Qualche riferimento di carattere personale, un indirizzo email privato simile a quello del presunto mittente, ed ecco depositato sui sistemi dell'azienda bersaglio un file contenente in realtà pericoloso malware. Le variazioni di uno scenario del genere sono davvero infinite ed è sufficiente solo un po' di creatività e di tempo per raccogliere le informazioni necessarie a lanciare una campagna di spear phishing efficace.

CARO AMICO TI SCRIVO: LE TRUFFE BEC

La **percentuale di successo** dei tentativi di spear phishing è in genere talmente **alta** da aver dato vita a una **categoria specifica di attacchi denominata BEC**, Business Email Compromise, che sfrutta l'ingegneria sociale per spingere le vittime a **effettuare spontaneamente operazioni a beneficio del cybercriminale** di turno.

I messaggi BEC **impersonano un contatto di lavoro** (un collega, un dirigente, un fornitore, uno studio legale, un'autorità...) con l'obiettivo di dare corso a mandati di pagamento non dovuti, dirottare pagamenti legittimi su un conto bancario controllato dal truffatore, fornire informazioni rivendibili nel dark web oppure utili ad azioni di spionaggio industriale e così via.

Gli attacchi BEC (o "truffa del CEO") **risultano particolarmente efficaci perché sono realizzati in modo da superare i filtri antivirus e antispam** in quanto non contengono alcun allegato e non arrivano mediante invii di massa: anzi, per loro stessa natura presentano un grado di personalizzazione molto elevato e accurato.

Non è un caso che negli ultimi tempi le vittime di attacchi BEC – aziende grandi e piccole così come enti pubblici, scuole e ospedali – compaiano sempre più frequentemente sui media: chi ha creduto di **saldare un fornitore**, chi invece ha dato corso a un **pagamento** presumibilmente **richiesto dall'amministratore delegato**.

Le aziende rappresentano un bersaglio decisamente appetitoso per i cybercriminali sia per le potenzialità che esse offrono, sia per l'ampia superficie di attacco direttamente proporzionale al numero di dipendenti che vi lavorano.

Paradossalmente, un attacco BEC è forse quello che crea meno problemi a chi ne viene colpito. Certo, il danno finanziario può essere rilevante (se nel 2018 la S.S. Lazio ha perso 2 milioni di euro, l'anno successivo Maire Tecnimont ne ha persi ben 172, solo per restare in Italia), ma il tutto si esaurisce nella sottrazione di denaro. Ben più gravi possono essere invece le **conseguenze del phishing quando l'obiettivo è quello di infettare i sistemi informatici di un'azienda con il ransomware**, un particolare tipo di malware che **crittografa tutti i file** che incontra propagandosi dal dispositivo originario alle cartelle condivise e man mano a tutti i PC e server collegati alla stessa rete interna. I file crittografati rimangono a tutti gli effetti inaccessibili **fintanto che non venga pagato un riscatto** per ottenere la chiave di decifrazione che, teoricamente, consentirebbe il ripristino dei file stessi.

Pagare soldo, vedere cammello...: conviene pagare il riscatto?

Il versamento del riscatto non costituisce tuttavia garanzia di recupero dei file cifrati: innanzitutto i tempi concessi per pagare (solitamente attraverso bitcoin o altre criptovalute) sono molto stretti, e questo rappresenta un serio problema nelle organizzazioni che richiedono diversi livelli di autorizzazione prima di poter decidere un'operazione del genere, senza considerare il fatto che solamente dotarsi di criptovalute implica per un'azienda il superamento di una serie di ostacoli tecnici, operativi, burocratici e financo fiscali e normativi.

In secondo luogo, **non sempre il responsabile dell'attacco ransomware è di parola**, come possono testimoniare le aziende che non hanno ricevuto la chiave promessa o ne hanno ricevuta una inutile (anche con le migliori intenzioni, può infatti bastare un bug nel ransomware per rendere impossibile il recupero dei file).

Infine, i **sistemi informatici di produzione**, quelli che per intenderci non smettono mai di svolgere il proprio lavoro, **possono essere comunque irrecuperabili**. Pensiamo ai file associati a un database transazionale che continua a essere utilizzato anche dopo l'attacco del ransomware: in questo caso il file che si proverà a ripristinare una volta ottenuta la chiave si troverà in uno stato differente da quello in cui era stato cifrato, rendendo vana la procedura.

Le conseguenze di un ransomware possono essere quindi molto gravi, con **fermi operativi prolungati** per giorni o settimane. In casi estremi, ma non impossibili, **si può arrivare anche a chiudere del tutto i battenti**, come è stata costretta a fare a fine 2019 una società di telemarketing dell'Arkansas che pure aveva pagato il riscatto richiesto e ricevuto la chiave di decifrazione. [1]

La diffusione del fenomeno sta inoltre spingendo molti legislatori ad assumere misure che ricordano quelle adottate in Italia a partire dagli anni Settanta del secolo scorso in conseguenza delle ondate di rapimenti che hanno costellato le cronache di quel periodo: nello Stato di New York sono stati presentati a inizio 2020 due disegni di legge che intendono **vietare il pagamento di riscatti per il ransomware**, almeno da parte degli enti pubblici,[2] mentre altrove ci si interroga sempre più spesso se non sia opportuno impedire a chiunque di cedere alle richieste dei cybercriminali nella speranza che la chiusura del rubinetto dei pagamenti si traduca nella scomparsa del fenomeno. La questione è ovviamente molto complessa e se ne sentirà parlare ancora a lungo.

UNA VIA D'USCITA

La complessità degli attacchi di phishing nasce dalla loro caratteristica di **unire la componente tecnologica a quella umana** costringendoci a intervenire su due tavoli differenti se vogliamo neutralizzare le minacce attuali e le relative evoluzioni che prevedibilmente emergeranno nel prossimo futuro.

Misure difensive tecniche sono tanto necessarie – almeno come prima linea di protezione – quanto efficaci; d'altra parte non sono sufficienti.

Si tratta di una situazione assolutamente speculare rispetto a quella degli attaccanti: **alle loro armi informatiche dovremo reagire con strumenti informatici**, mentre **ai loro tentativi di ingannare gli interlocutori** tramite azioni di ingegneria sociale **dovremo rispondere facendo trovare loro persone preparate** e non disposte a cadere in trappole congegnate in modo più o meno efficace.

Iniziamo dall'IT, dunque. Diamo per scontato che entrati nel terzo decennio del XXI secolo non vi siano più aziende prive di protezioni basilari realizzate per mezzo di **firewall di rete e di antivirus** attivi sui PC e su ogni altro dispositivo connesso.

Se questo non fosse il tuo caso interrompi momentaneamente la lettura di questo white paper, procurati *subito* un firewall e un antivirus, e quindi torna qui per conoscere i passi successivi.

---

1 https://www.zdnet.com/article/company-shuts-down-because-of-ransomware-leaves-300-without-jobs-just-before-holidays/
2 https://gdpr.report/news/2020/01/28/privacy-ny-state-wants-to-ban-paying-ransomware-demands

Fatto? Bene, proseguiamo.

Cosa succede quando abbiamo timore che qualcuno possa cercare di entrare in casa nostra forzando la porta di ingresso?

Ovviamente ricorriamo a una porta blindata e a un allarme. Lo stesso dobbiamo fare con la nostra **posta elettronica**, che possiamo **irrobustire per mezzo di un apposito filtro**. Attenzione, non ci riferiamo qui ai tradizionali filtri antispam, soluzioni basate su regole e sostanzialmente statiche.

I **filtri moderni** progettati per le minacce attualmente in circolazione, phishing compreso, sono invece in grado di fare molto di più individuando mittenti fraudolenti, falsificazione di messaggi, indirizzi apparentemente simili a quelli legittimi, e presenza di link pericolosi e allegati incoerenti con gli altri contenuti delle mail.

Strumenti di questo tipo hanno una **natura dinamica e sfruttano le potenzialità dell'intelligenza artificiale** per tenere il passo con l'evoluzione degli attacchi; nel malaugurato ma sempre possibile caso in cui qualche messaggio dovesse riuscire comunque a passare, l'aggiunta di un **sistema di controllo della navigazione** – evoluzione dei cosiddetti *filtri parentali* diffusi da almeno vent'anni – potrà verificare la qualità dei link selezionati dagli utenti intercettando tempestivamente l'eventuale redirezione verso siti illegittimi o pericolosi.

Dalle contromisure puramente tecniche e sostanzialmente invisibili agli utenti dobbiamo poi passare agli **accorgimenti ibridi**, ovvero quelle soluzioni IT che mettono a disposizione dell'utilizzatore le informazioni che gli sono necessarie per tenere un comportamento prudente.

Pensiamo per esempio ai programmi di posta elettronica, dove negli anni un malinteso senso di semplificazione della cosiddetta "*user experience*" (ovvero il sistema complessivo di interfaccia del software) ha condotto a un progressivo **nascondimento di dati che oggi si scoprono essenziali** per poter valutare con certezza la qualità dei messaggi email ricevuti.

È infatti molto facile **falsificare il nominativo del mittente** che viene normalmente visualizzato all'apertura di un messaggio o nell'indice delle email ricevute; tuttavia, ogni email è accompagnata da una serie di informazioni tecniche, raggruppate nel relativo ***header***, dove compare il reale, effettivo indirizzo dal quale è stato spedito il messaggio.

Un programma di posta che permetta di **visualizzare facilmente anche questo campo** offre un aiuto davvero prezioso per l'utente che sia stato adeguatamente sensibilizzato sul tema.

E proprio la sensibilizzazione degli utenti è la chiave di volta di una difesa a prova di bomba.

Pensiamoci un attimo: in buona parte il phishing ha successo perché coglie le proprie vittime del tutto impreparate di fronte a comunicazioni camuffate da richieste legittime – una situazione che ricorda quella dei truffatori porta a porta che si spacciano per tecnici del gas o messi comunali.

Tanto nel mondo reale che in quello online, **essere consapevoli dell'esistenza del fenomeno è la prima regola** per evitare di cadere in trappola. Come lo si fa? Con l'informazione e la formazione, assicurandosi che i **dipendenti delle aziende non solo rimangano aggiornati** sull'evoluzione di tentativi di attacco, ma che **siano ben consci dell'impatto** che il comportamento superficiale di un solo individuo – nella propria sfera professionale così come anche in quella personale – può avere sull'intera organizzazione.

Una buona idea è quella di accompagnare le iniziative di sensibilizzazione con periodiche **campagne di phishing simulato** che permettano di misurare con dati reali l'efficacia delle azioni preventive realizzate fino a quel momento: una conferma sul campo del grado di prontezza che l'azienda può dispiegare a fronte di tentativi di attacco.

E per quanto riguarda le famigerate **truffe BEC**, non si può evitare di notare come molti casi finiti sui giornali si sarebbero potuti evitare in presenza di adeguate **procedure organizzative**.

La variazione dell'IBAN di un fornitore, l'emissione di un mandato di pagamento, la comunicazione di dati sensibili o informazioni di natura critica per l'attività aziendale dovrebbero seguire un iter formale appositamente studiato per evitare che la leggerezza del singolo possa danneggiare l'azienda nel suo complesso.

Non si tratta di aggiungere uno strato di burocrazia fine a se stessa, quanto di estendere a un nuovo campo di sfide emergenti tutti quei processi e accorgimenti che da sempre circondano le operazioni critiche di qualsiasi organizzazione come quelle di tesoreria.

Soprattutto per le PMI più piccole e meno strutturate, che spesso lasciano queste procedure all'iniziativa personale del responsabile di turno, può essere una preziosa occasione per iniziare a **dotarsi di strumenti organizzativi** che, anche al di là del phishing, sono essenziali per una migliore gestione complessiva del business.

Glossario

BEC Business Email Compromise – Una sofisticata truffa mirata che nella sua versione più diffusa assume l'aspetto di comunicazioni provenienti da un dirigente aziendale per convincere un altro dipendente a dare corso a pagamenti verso conti bancari riconducibili agli autori dell'illecito. Per dare credibilità alle richieste vengono spesso falsificati documenti ufficiali e creati domini Internet dal nome molto simile a quello delle aziende e degli enti coinvolti.

Dark web – Un vero e proprio web parallelo costituito da sistemi collegati a Internet attraverso software e configurazioni particolari, al cui interno si svolgono attività prevalentemente illegali di ogni genere. Il dark web rappresenta una componente del cosiddetto deep web, ovvero quella porzione del web che non è accessibile ai normali motori di ricerca.

DDoS – Distributed Denial of Service – Un attacco rivolto contro un sistema che viene contemporaneamente contattato con richieste di accesso o di traffico da migliaia di computer e dispositivi connessi al solo scopo di saturare la banda di comunicazione disponibile in modo da rendere inutilizzabile il sistema stesso. Nel Dark Web è possibile acquistare servizi DDoS gestiti da cybercriminali che controllano enormi quantità di computer (detti zombie) infettati da apposito malware quasi sempre veicolato mediante azioni di phishing.

Mining di criptovalute – La produzione di criptovalute come Bitcoin, Litecoin, Ethereum, Monero e altre è associata all'esecuzione di un massiccio quantitativo di calcoli matematici che richiede lunghi tempi di elaborazione da parte di un singolo computer. Per velocizzare queste operazioni e generare così nuove criptomonete, i cybercriminali sfruttano la potenza di calcolo di computer altrui su cui sia stato preventivamente installato del malware adeguato. Avendo a disposizione le risorse di calcolo di centinaia di migliaia o addirittura milioni di PC infetti, i cybercriminali possono arricchire la propria dotazione di criptovalute in tempi notevolmente ridotti.

Phishing – Una truffa diffusa principalmente tramite messaggi di posta elettronica e SMS attraverso i quali si tenta di carpire informazioni sensibili alle vittime facendo credere che la richiesta provenga da un interlocutore affidabile. I messaggi solitamente rimandano a pagine web fraudolenti che replicano l'aspetto di quelle ufficiali invitando il destinatario a inserire le proprie credenziali o i codici delle carte di credito con le scuse più diverse. A differenza delle truffe BEC, accuratamente personalizzate, il phishing si avvale di invii di messaggi in massa.

Ransomware – Un particolare tipo di malware che crittografa i file residenti sul computer colpito (e spesso anche su tutti gli altri dispositivi collegati alla stessa rete) che diventano così inaccessibili a meno di non pagare un riscatto per ottenere la chiave di decifrazione necessaria. Non sono rari i casi in cui anche la disponibilità di questa chiave non consenta il ripristino corretto dei sistemi, con gravi conseguenze per le aziende.

Spam – Messaggi indesiderati solitamente a carattere pubblicitario che rappresentano una porzione significativa del traffico mondiale di email. In molti Paesi l'invio di spam è reato e comunque quasi sempre contrario alle politiche d'utilizzo ammesse dagli Internet Service Provider. Per questo motivo, nonché per gli altissimi volumi di messaggi (anche alcuni miliardi) spediti da una normale campagna spam, i cybercriminali preferiscono effettuare l'invio attraverso computer di ignari utenti su cui sia stato precedentemente installato malware che ne permetta il controllo a distanza.

Spear phishing – Una variante del phishing estremamente personalizzata sul destinatario del tentativo di truffa. A differenza del normale phishing, i messaggi sono realizzati su misura dopo aver studiato il profilo della potenziale vittima attraverso le informazioni normalmente reperibili sul Web. Un accurato lavoro di preparazione permette di aumentare notevolmente l'efficacia dei messaggi prendendo alla sprovvista anche coloro che normalmente prestano poco credito alle comunicazioni indesiderate provenienti per posta elettronica.

Spyware – Una particolare tipologia di malware che ha lo scopo di raccogliere quante più informazioni possibili sull'utilizzatore del computer o del dispositivo sul quale risiede. A differenza del ransomware e di altri malware, lo spyware è scritto per restare ben nascosto più a lungo possibile raccogliendo dati sensibili che possono essere rilevati tramite sia la lettura dei file presenti sul sistema, sia il monitoraggio dei tasti premuti alla tastiera. Gli esemplari di spyware più sofisticati possono estendere il loro raggio d'azione anche alla rete alla quale è collegato il dispositivo infetto.