



**Adora ICT**  
CyberSecurity Linking Humans

## E-mail security

**Adora ICT**  
P.IVA 08590111004  
REA 1104976

Via Mosca 10 - 00142 (RM)  
Blend Tower  
Piazza Quattro Novembre 7 - 20124 (MI)

Mail [info@adora-ict.com](mailto:info@adora-ict.com)  
Telefono (+39) 06.43400115  
Fax (+39) 0643400118

# E-mail security

## Come proteggere il tuo business

**Uno strumento di lavoro può diventare una pericolosa minaccia per la sicurezza del tuo business.**

Nello svolgimento dell'attività aziendale, l'e-mail è uno degli strumenti quotidianamente più utilizzati ed il canale per il quale passa la maggior parte delle informazioni di business.

Proprio per questo motivo è anche il canale che i **cyber-criminali** utilizzano più spesso per attaccare l'organizzazione e le sue risorse.

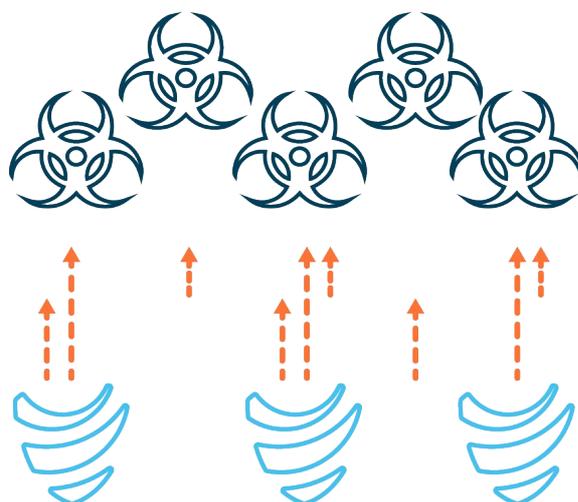
Ogni giorno il personale aziendale si trova a distinguere le e-mail utili da quelle indesiderate e disoneste preparate attraverso software automatici di compilazione, payload contenenti malware sempre più sofisticati, ecc...

### **La prassi non basta.**

Per tutelarsi dagli attacchi che possono incorrere sul web è certamente possibile applicare delle piccole accortezze come:

- non trasmettere dati ed informazioni sensibili
- non scaricare allegati presenti in email non richieste o inaspettate
- non cliccare link sconosciuti e verificare l'URL del sito dove l'e-mail vorrebbe reindirizzare.

Ciò nonostante i sistemi di sicurezza informatica manuali non sono in grado di tutelare il 100% della rete dalle moderne strategie di attacco.



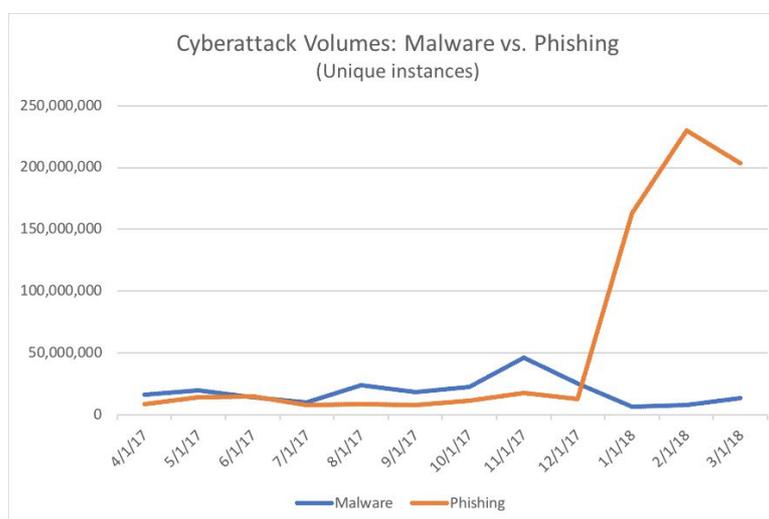
## Il rapporto Clusit

Il Clusit, l'Associazione italiana per la Sicurezza Informatica, ha definito il 2018 come l'anno peggiore di sempre in termini di sicurezza informatica. Il Phishing è stato nel 2018 la quarta tipologia di attacco più frequente ed ha registrato un aumento del 57% rispetto all'anno precedente. Mentre a livello globale, tra il 2018 e 2019, gli attacchi significativi sono cresciuti del 38%. Crescono anche le minacce alle istituzioni ma gli attacchi "multiple target", attacchi che non si rivolgono ad un settore specifico ma a più comparti contemporaneamente, rimangono la prima tipologia di aggressione con 304 attacchi nel 2018.

TECNICHE DI ATTACCO PER TIPOLOGIA	2014	2015	2016	2017	2018	2018 su 2017	Trend
Malware	127	106	229	446	585	31,2%	↗
Unknown	199	232	338	277	408	47,3%	↗
Known Vulnerabilities / Misconfig.	195	184	136	127	177	39,4%	↗
Phishing / Social Engineering	4	6	76	102	160	56,9%	↗
Multiple Techniques / APT	60	104	59	63	98	55,6%	↗
Account Cracking	86	91	46	52	56	7,7%	↗
DDoS	81	101	115	38	38	0,0%	=
0-day	8	3	13	12	20	66,7%	↗
Phone Hacking	3	1	3	3	9	200,0%	↗
SQL Injection	110	184	35	7	1	-85,7%	↘

Fonte: Rapporto Clusit 2019

Nel 75% degli attacchi verso questa categoria, il cybercrime ha utilizzato tecniche altamente industrializzate, pensate per ottenere il maggior numero di successi in situazioni diverse.



## Non solo spam.

Le tipologie di attacco che possono essere veicolate tramite e-mail sono molteplici.

Lo **Spam** propone servizi non richiesti o cela vere e proprie truffe ma generalmente colpisce l'utente privato e non le organizzazioni aziendali. È la tipologia di attacco più frequente e per questo la più conosciuta ma è anche la più innocua.

Il **Phishing** inganna le sue vittime sfruttando l'attendibilità di una fonte accreditata.

Il vero mittente del messaggio viene celato dietro il nome di una società legittima, un istituto di credito, un ente o un'azienda terza notoriamente conosciuta. Il contenuto del messaggio spinge il destinatario a cliccare su un link ed eseguire involontariamente il download di un malware. Questi link possono anche condurre il malcapitato su un sito web clone di quello che gli hacker hanno utilizzato come esca, rendendo di fatto l'attacco ancora più efficace.



Lo **Spear Phishing** si focalizza su una vittima specifica (organizzazione o persona).

L'e-mail viene personalizzata rispetto al destinatario per celare ancor meglio la sua natura fraudolenta. All'occhio dell'utente risultano molto meno ingannevoli e la truffa è più efficace.

Il **Whaling** è un attacco rivolto principalmente ai livelli dirigenziali. Ad esempio il messaggio potrebbe richiedere un pagamento verso conti bancari non intestati a società creditrici dell'azienda.

## Le nostre soluzioni

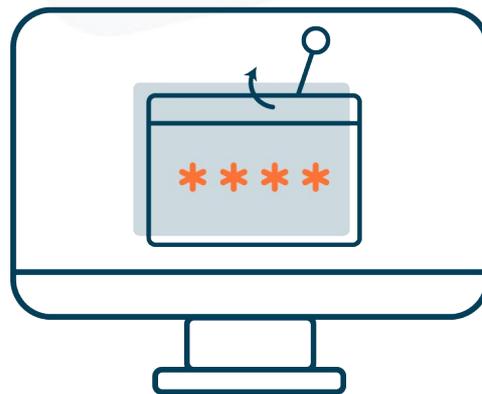
Per difendere l'azienda dal **Phishing**,  
**Adora-ICT** propone una soluzione attiva sia  
sul fronte tecnico che sulle risorse umane.

### Azione diretta

Proteggere il server aziendale installando  
un software specializzato, in grado di filtrare  
le e-mail pericolose. Grazie a tecnologie di  
**machine learning** e **AI**, il software riconosce  
minacce sia nei messaggi di testo sia in messaggi  
contenenti attachment.

### Azione indiretta

Educare le risorse che quotidianamente hanno contatto con il canale.  
Agire sul personale instillando maggiore consapevolezza verso i rischi che si corrono  
nell'interazione con le tecnologie digitali e nello specifico per questo tipo di attacco, permette  
di adeguare il loro comportamento alla necessità di protezione dell'organizzazione  
e alle sfide imposte dall'evoluzione del crimine informatico.



**Non piove più sul bagnato.  
Un sistema sicuro ti mette al riparo da molti rischi.**

**CONTATTACI PER UN APPUNTAMENTO**

**Info Line:** 06.43400115

**Informazioni generali ed amministrazione:** [info@adora-ict.com](mailto:info@adora-ict.com)

**Sicurezza:** [sec.sales@adora-ict.com](mailto:sec.sales@adora-ict.com)

## I nostri partner



kaspersky

tenable

WatchGuard

Barracuda  
Your journey, secured.



LIBRAESVA  
certified partner

Microsoft

CYBERA

DATACORE



VEEAM  
PROPARTNER

CITRIX

## Le nostre certificazioni



CEH  
Certified Ethical Hacker



Microsoft  
CERTIFIED  
Professional

Microsoft  
CERTIFIED  
Technology Specialist

CEI  
Certified EC-Council Instructor



PMI  
Project Management Institute

COBIT  
AN ISACA FRAMEWORK



SOPHOS  
Certified Engineer

ITIL  
Foundation V3





Via Mosca 10, 00142 Roma  
Blend Tower - Piazza Quattro Novembre 7, 20124 Milano

**Info Line:**  
Tel. 0643400115  
Fax: 064340018

[info@adora-ict.com](mailto:info@adora-ict.com)

---

© Adora ICT - 2019 P.IVA 08590111004 / REA 1104976