



DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE ON CONSUMER POLICY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

Task Force on Spam

LE "BEST PRACTICES" DI BIAC e MAAWG PER GLI INTERNET SERVICE PROVIDERS (ISP) E GLI OPERATORI DI RETE

Traduzione (non-ufficiale) in italiano del documento "BIAC-MAAWG Best Practices for Internet Service Providers and Network Operators". Si ringrazia il [Ministero per l'Innovazione e le Tecnologie](#) italiano per la traduzione del presente documento.

*Italian translation (unofficial) of the BIAC-MAAWG Best Practices for Internet Service Providers and Network Operators.
We wish to thank the Italian Minister of Innovation and Technologies for the translation of this document.*

© OECD / OCDE 2006.

LE "BEST PRACTICES" DELLA BIAC PER GLI INTERNET SERVICE PROVIDERS (ISP) E GLI OPERATORI DI RETE

Introduzione

1. Gli ISP e i network operators rivestono un importante ruolo nella lotta allo spam.
2. Data l'importanza di tale ruolo, gli ISP, i network operators, i gruppi e le associazioni tecniche continuano a condividere le best practices per la prevenzione/riduzione dello spam inviato da/attraverso le proprie reti.
3. Anche se le best practices non costituiscono, da sole, una soluzione esauriente per combattere il fenomeno dello Spam, fanno parte di una strategia di più vasto respiro. L'efficacia delle pratiche comuni sarà proporzionale al numero degli enti che le sostiene e applica.
4. L'impatto positivo derivante dall'adozione delle Best Practices volontarie da parte degli ISP e degli Operatori di Rete sarà amplificato se anche gli utenti prenderanno i provvedimenti necessari per la protezione e la sicurezza dei loro computer, dei software e delle reti, inclusa la protezione della loro identità personale online.

Scopo

5. Le Best Practices della BIAC per gli ISP e gli Operatori di Rete sono dei principi sviluppati su base volontaria dalle aziende al fine di migliorare la sicurezza infrastrutturale della rete nella lotta allo Spam. Il mondo industriale continuerà a collaborare per lo sviluppo di ulteriori misure tecniche e procedurali per la completa attuazione di tali principi.
6. LA BIAC propone le seguenti Best Practices agli ISP e agli Operatori di Rete quale importante strumento nella battaglia allo Spam.
7. Tali Best Practices ed eventuali ulteriori provvedimenti sono volontari, e le aziende devono dare priorità ai quadri legislativi e normativi vigenti.
8. L'attuazione delle Best Practices e di qualsiasi ulteriore provvedimento varierà in base alle configurazioni tecniche dei singoli provider/operatori di rete e delle loro particolari esigenze e sfide di business.
9. La flessibilità nell'attuazione delle Best Practices e di qualsiasi ulteriore provvedimento rappresenta un elemento chiave per un'adozione ampia e significativa da parte dei provider di servizi. Data la rapidità dei cambiamenti tecnologici, le Best Practices verranno riviste e aggiornate periodicamente.

LE BEST PRACTICES

Contesto/Definizioni

10. Sotto qualsiasi giurisdizione nazionale, le Best Practices vengono consigliate solo se non entrano in conflitto con la legislazione nazionale vigente.
11. Nel contesto di queste Best Practices per "ISP" e "Operatore di Rete" si intende qualsiasi ente che operi un server SMTP collegato a Internet.

La BIAC consiglia agli ISP e agli Operatori di Rete di:

1. Eliminare l'attrezzatura degli utenti finali compromessa, nonché gli elementi di rete, quali fonti di Spam. Tale processo tempestivo avverrà nel rispetto dei limiti del rilevante quadro legislativo.
2. Attuare l'autenticazione della posta elettronica quanto prima.
3. Bloccare gli allegati elettronici potenzialmente infettivi. Nel caso di un filtraggio della posta elettronica o di allegati con contenuto d'autore, va stabilito un accordo a priori con il consumatore nel rispetto del quadro legislativo vigente.
4. Controllare attivamente il volume del traffico email in entrata e in uscita per individuare attività di rete insolita nonché la fonte di tale attività, e reagire adeguatamente.
5. Istituire adeguati processi intra-aziendali per la pronta reazione a eventuali rapporti su incidenti di altri operatori di rete, anche accettando lamentele da parte degli utenti finali.
6. Notificare agli abbonati, insieme ai provider di posta elettronica per le aziende, le proprie politiche e procedure di sicurezza.
7. Inviare notifiche di non consegna (NDN) esclusivamente per quanto riguarda i messaggi originati dai propri titolari di casella elettronica.
8. Prendere i provvedimenti necessari perché solo gli utenti autorizzati utilizzino gli email *submit servers*.
9. Assicurarsi che tutti i nomi a dominio, gli archivi del Sistema di Nome a Dominio (DNS) e le rilevanti registrazioni di indirizzi Internet protocol (IP) (ad es. WHOIS, Shared WHOIS Project [SWIP] o referral WHOIS [RWHOIS]) siano gestiti in modo responsabile con informazioni corrette, complete e attuali, e che tali informazioni includano punti di contatto per il personale responsabile per la risoluzione dei fenomeni di cattivo uso di indirizzi postali, numeri telefonici, indirizzi di posta elettronica, ecc.
10. Assicurarsi che i propri indirizzi pubblicamente *routable* e che gli indirizzi IP visibili da Internet abbiano dati DNS *forward* e *reverse*, oltre che dati WHOIS e SWIP, aggiornati e appropriati; che tutti gli operatori di reti locali (LAN) siano conformi alle Request for Comments (RFCs) 1918 - "Address Allocation for Private Internets," e che in particolare le LAN non utilizzino spazio registrato globalmente a nome di qualcun altro, o spazio non registrato a nome di nessuno, quale spazio privato IP.