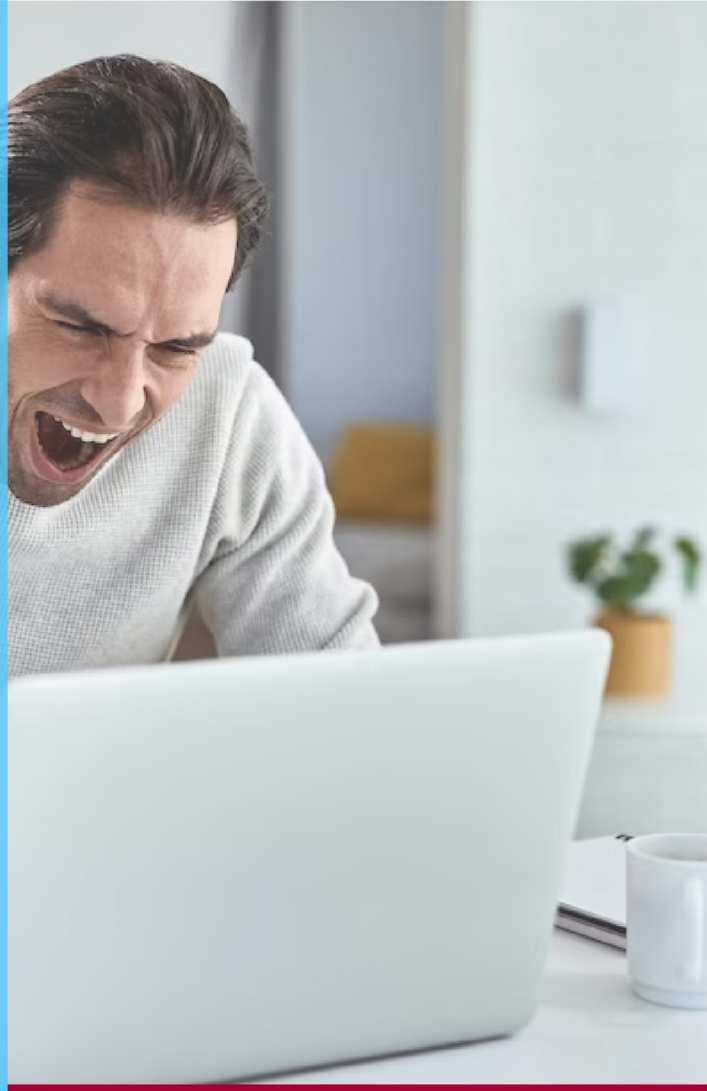
Qweb

A TECHONE COMPANY



HOSTING - NIEUWS

DKIM/DMARC/SPF

Wat te doen tegen scammers, spoofers en ander mail-abuse

1 SEPTEMBER

Q-FILTER

WAT KAN JE ERMEE?

FAIL!

SOFT OF HARD?

WAT TE DOEN

TEGEN SCAMMERS, SPOOFERS EN ANDERE MAIL-ABUSE?

Hoewel email een onmisbaar communicatiemiddel is geworden, brengt het ook de nodige gevaren en risico's met zich mee die zo nu en dan de nodige aandacht verdienen. Zo kun je te maken krijgen met scammers, spoofers en andere vormen van mail abuse. Maar hoe ga je hier precies mee om?

Deze maand gaan we je bijpraten over hoe je jouw email op de meest veilige manier kunt gebruiken en kunt beschermen tegen gevaren van buitenaf.

#LetsMakeHostingWork #email #phishing #abuse

Q-FILTER, WAT KAN JE ERMEE?

Het kan je zomaar overkomen; je zit achter je computer/ laptop of telefoon en je ontvangt een mail van de bank die vraagt om je gegevens te veranderen. Zonder dat je er over nadenkt geef je jouw gegevens door aan de bank, althans, dat denk je op dat moment. De gevolgen worden later duidelijk. 1 kleine fout die je hebt gemaakt leidt nu tot ernstige financiële gevolgen.

Hoe had je dit kunnen voorkomen? Phishing mails zien er steeds 'echter' en professioneler uit en lijken sterk op de mails die je herkent van jouw bank. Door middel van het Q-filter van Qweb wordt er een slimme technologie toegepast om alle inkomende e-mail te filteren en spam te elimineren alvorens deze in jouw mailbox terecht komen. De werking van Q-filter is vrij simpel: eerst worden alle verzonden mails op het Q-filter-cluster opgevangen, vervolgens onderzoekt het Q-filter direct of deze e-mailberichten onder spam vallen. Het Q-filter erkent en elimineert direct nieuwe spamberichten en zorgt ervoor dat deze niet door de spamfilter heen glippen. Alle schone e-mails worden vervolgens in jouw mailbox afgeleverd.

Wil je ook gebruik maken van het Q-filter? Of wil je hier meer informatie over ontvangen?
Neem dan gerust contact met ons op.

FAIL! SOFT OR HARD?

SPF, oftewel Sender Policy Framework, is een authenticatiemethode die wordt gebruikt om te voorkomen dat spammers valse e-mails versturen vanuit jouw domein. Een SPF-record is in wezen een lijst van servers die gemachtigd zijn om namens jouw domein e-mails te verzenden.

Een correct geconfigureerd SPF-record kan je e-mailbezorgbaarheid aanzienlijk verbeteren. E-mailontvangers zoals Gmail, Outlook en Yahoo voeren SPF-controles uit. Als een e-mail wordt verzonden vanaf een server die niet op de SPF-lijst staat, kan deze als verdacht worden gemarkeerd of zelfs worden geblokkeerd.

SOFTFAIL VS HARDFAIL IN SPF-RECORDS:

Softfail (~all)

Voordelen:

- Flexibiliteit: Biedt ruimte voor onzekerheid over alle servers die e-mails namens jouw domein kunnen verzenden.
- Minder disruptief: Minimaliseert de kans dat legitieme e-mails tijdens de testfase worden geblokkeerd.

Nadelen:

- Minder veilig: Mogelijk bezorging van phishing-pogingen of ongewenste e-mails in de spamfolder.

Hardfail (-all)
Voordelen:

- Strikte beveiliging: E-mails die niet van gespecificeerde servers komen, worden resoluut geweigerd.

Nadelen:

- Risico op weigering van legitieme e-mails: Kan communicatieproblemen veroorzaken als het SPF-record niet correct is geconfigureerd.

Een praktijkvoorbeeld illustreert het belang hiervan: Stel je voor, je ontvangt een e-mail van wat lijkt een collega te zijn, met een verzoek om een document te openen. In werkelijkheid komt het van een hacker die het e-mailadres van je collega heeft nagebootst. Met een goed SPF-record zou deze phishing-poging kunnen worden gestopt.

Dus, softfail of hardfail? De keuze hangt af van je bereidheid om risico's te nemen. Qweb staat klaar om je te helpen en adviseren met het correct gebruik van je SPF-record, zodat je beschermd blijft en je e-mails de juiste bestemming bereiken.