

ALLES KAN BETER

Spam... Een paar jaar geleden bestond het niet eens, nu heeft iedereen er de buik van vol. Af en toe eens wat reclame krijgen in je mailbox is nog aanvaardbaar, maar als je meer ongewenste post krijgt dan goedbedoelde mails, dan is de fun er snel af. En nog erger wordt het als jouw gegevens bij mensen met echt slechte bedoelingen terecht komen, en ze die gaan gebruiken om via *phising* aan je bankgegevens te geraken. Of als grote mailleveranciers goedbedoelde mails van jouw vereniging zonder boe of ba gaan wegslijten omdat ze denken dat het over spam gaat.

Dat kan beter! We zetten hieronder een aantal dingen op een rij die allemaal een klein beetje helpen om het spam-probleem in te dijken. Ook tips voor de gewone internetgebruiker, want behalve webmasters dragen ook zij een deel van de verantwoordelijkheid. Weg met die spam!

TIPS VOOR WEBMASTERS

Beveilig links met e-mailadressen

Uit recent onderzoek blijkt dat pc's die zonder firewall op het internet worden aangesloten na gemiddeld twaalf minuten opgespoord zijn door spyware-robots of botnets. Voor websites is dat niet anders. Van zodra je een site publiceert, springen tientallen robots op je code op zoek naar allerlei interessante informatie.

Om te voorkomen dat je mailadressen binnen de kortste keren in allerlei spamlijsten zitten, is het belangrijk dat je deze adressen beveiligt. Gewoon

```
<p>Mail naar <a href="mailto:info@scoutnet.be" title="Mail naar Scoutnet">info@scoutnet.be</a>.</p>
```

schrijven laat de robots immers toe om zonder moeite je e-mailadres in te lezen en er nadien spam naartoe te sturen.

De maillinks beveiligen, kan op verschillende manieren, maar bijna altijd door gebruik van Javascript.

1. Enkel Javascript: de meest eenvoudige manier is om in een *a*-tag het e-mailadres op te splitsen en door Javascript weet te laten samenstellen. Dat kan met volgend scriptje:

```
<p>
  Mail naar
  <script type="text/javascript">
    <!--
    document.write('<a href="mailto:info">');
    document.write('@');
    document.write('scoutnet.be" title="Mail naar Scoutnet">');
    document.write('info');
    document.write('@');
    document.write('scoutnet.be');
  </script>
```

```

    document.write('</a>');
    //-->
</script>
.
</p>

```

2. Nog eens Javascript: De methode is gelijkaardig als hierboven, maar deze keer proberen we de link een beetje te coderen, zodat het e-mailadres niet rechtstreeks valt uit te lezen. Je krijgt dan iets als dit:

```

<p>
  Mail naar
  <script type="text/javascript">
    eval(unescape( '%76%61%72%20%73%3D%27%61%6D%6C%69%6F%74%69%3A%
    66%6E%40%6F%63%73%75%6F%6E%74%74%65%62%2E%22%65%74%20%74%69%65%
    6C%22%3D%61%4D%6C%69%6E%20%61%61%20%72%63%53%75%6F%6E%74%74%65%
    22%27%3B%76%61%72%20%72%3D%27%27%3B%66%6F%72%28%76%61%72%20%69%
    3D%30%3B%69%3C%73%2E%6C%65%6E%67%74%68%3B%69%2B%2B%2C%69%2B%2B%
    29%7B%72%3D%72%2B%73%2E%73%75%62%73%74%72%69%6E%67%28%69%2B%31%
    2C%69%2B%32%29%2B%73%2E%73%75%62%73%74%72%69%6E%67%28%69%2C%69%
    2B%31%29%7D%64%6F%63%75%6D%65%6E%74%2E%77%72%69%74%65%28%27%3C%
    61%20%68%72%65%66%3D%22%27%2B%72%2B%27%22%3E%69%6E%66%6F%40%73%
    63%6F%75%74%6E%65%74%2E%62%65%3C%2F%61%3E%27%29%3B' ) )
  </script>
.
</p>

```

Op www.antispam.de/encoder.php vind je een scriptje om e-mailadressen op deze manier te versleutelen.

3. Javascript in combinatie met PHP: deze methode werkt op dezelfde manier als de eerste oplossing, maar probeert het de webmaster iets gemakkelijker te maken. In plaats van overall waar je een e-mailadres wil schrijven het volledige Javascript te kopiëren, maken we hier gebruik van een zelfgemaakte PHP-functie:

```

<?php
function geefVeiligMailadres($emailadres,$titel) {
    $titel = addslashes($titel);
    $mailrij = explode("@", $emailadres);
    $veiligadres = "<script type=\"text/javascript\">";
    $veiligadres .= "\n <!--";
    $veiligadres .= "\n document.write('<a href=\"mailto: \"
    . $mailrij['0'] . \"');";
    $veiligadres .= "\n document.write('@');";
    $veiligadres .= "\n document.write('\" . $mailrij[\"1\"
    . \"\" title=\"\$titel\">');";
    $veiligadres .= "\n document.write('\" . $mailrij[\"0\"
    . \"');";
    $veiligadres .= "\n document.write('@');";
    $veiligadres .= "\n document.write('\" . $mailrij[\"1\"
    . \"');";
    $veiligadres .= "\n document.write('</a>');";
    $veiligadres .= "\n //-->";
    $veiligadres .= "\n</script>";
    return $veiligadres;
}
?>

```

Deze zet je best in een apart bestandje dat je include op elke pagina waar je een e-mailadres veilig wil weergeven. Op de pagina zelf zet je dan:

```
<p>Mail naar <?php echo(geefVeiligMailadres("info@scoutnet.be", "Mail naar Scoutnet")); ?>.</p>
```

of

```
<?php
echo("<p>Mail naar " . geefVeiligMailadres("info@scoutnet.be",
"Mail naar Scoutnet") . "</p>");
?>
```

4. Zonder @: een eenvoudige oplossing is om het "@"-teken en elk puntje te vervangen door voluit geschreven woorden. Zo heeft de robot helemaal niet door dat er een mailadres staat. Je krijgt dan:

```
<p>Mail naar info at scoutnet punt be.</p>
```

Het nadeel hierbij is dat bezoekers niet meer op een link kunnen klikken. Als het een lang e-mailadres is, bestaat de kans dat ze typfouten maken.

5. Opzettelijk verkeerd: schrijf met opzet het e-mailadres achterstevoren:

```
<p>Mail naar <a href="mailto:be.scoutnet@info" title="Mail naar Scoutnet">be.scoutnet@info</a>.</p>
```

Zorg wel dat je dit duidelijk maakt aan je bezoekers, zodat ze weten dat ze het nog moeten omdraaien. Of maak gebruik van CSS om het toch in de normale leesrichting weer te geven. Zie www.cssplay.co.uk/menu/email.html.

6. Opzettelijk onbruikbaar maken: voeg met opzet een woord toe tussen de domeinnaam en het topdomein:

```
<p>Mail naar <a href="mailto:info@scoutnet.DOEDITWEG.be" title="Mail naar Scoutnet">info@scoutnet.DOEDITWEG.be</a>.</p>
```

7. In een afbeelding: maak een afbeelding van je e-mailadres, zoals bijvoorbeeld de e-mailadressen op www.dns.be/nl/home.php?n=6.
8. Zonder *mailto*: een laatste manier ten slotte is het vermijden van mailadressen. Dat los je dan op door te werken met een mailformulier. Zo hoef je het e-mailadres niet te publiceren en kunnen je bezoekers zich toch richten tot specifieke ontvangers. Let hierbij wel op het gebruik van robotbestendige formulieren (zie hieronder).

Gebruik robotbestendige formulieren

Niemand heeft graag berichten op zijn gastenboek die uitpuilen van links naar pornosites of andere rommel. Met een paar tips maak je het robots lastiger om daar in te slagen:

1. Gebruik een *captcha*: een bevestigingscode die in een afbeelding verwerkt zit. Zorg er wel voor dat op de captcha voldoende storing zit (lijnen, verkleurende

achtergronden), want sommige bots hebben OCR-ondersteuning zodat ze ook teksten in een afbeelding kunnen inlezen.

2. Geef je gastenboek niet de naam *guestbook.php* of *gbook.php*. Met de Nederlandstalige benaming gaat het al veel beter. En een nietszeggende paginanaam verkleint de kans nog wat.
3. Doe een controle op de ingevoerde velden: kijk na of het om een mailadres gaat en of er geen newlines ("\n") in voorkomen. Beperk eventueel het toegelaten aantal karakters per veld. Je kan ook alle HTML-tags uit het bericht filteren vooraleer het verder te verwerken (met *strip_tags(\$variabele)* in PHP). Meer info hierover vind je op <http://test.scoutnet.be/mail/spamform.php>.
4. Voorkom *MySQL-injection* door in een variabele vóór alle aanhalingstekens een slash te zetten vooraleer de variabele in de database te steken. In PHP kan je daarvoor *addslashes(\$variabele)* gebruiken.
5. Registreer de IP-adressen wanneer een bericht gepost wordt. Blijkt het om een spambot te gaan, dan kan je het in een blacklist zetten zodat geen tweede keer meer onder hetzelfde adres kan gepost worden.
6. Maak een lijst met "verboden" woorden. Wordt een bericht met het woord "viagra" gepost, dan kan je een scriptje zo schrijven dat de post geweigerd wordt. Hetzelfde kan je doen voor onbestaande of "illegale" domeinnamen die in e-mailadressen gebruikt worden.

Er is nog een andere manier waarop je formulier een bedreiging kan zijn. Misschien gebruik je een contactformulier waarbij na het klikken op de verzendknop een mailtje gestuurd wordt naar de ontvanger? Dan bestaat de kans dat dit misbruikt wordt om spam te sturen, en wel naar veel meer mensen dan alleen naar de ontvanger van het bericht.

De oplossing voor dit probleem bestaat erin een doorgedreven controle te doen op de ingevoerde velden. Een ingevoerd e-mailadres kan je bijvoorbeeld als volgt testen op geldigheid:

```
<?php
if (isset($_POST['email'])) {
    $email = $_POST['email'];
} else {
    $email = "";
}

$fout = "";

if ($email == "") {
    // het veld "email" werd leeggelaten
    $fout .= "\n <li>Er werd geen e-mailadres ingevoerd.</li>";
} else {
    // kijk na of er niet-toegelaten karakters werden ingevoerd
    $email2 = ereg_replace("@", "!", "$email");
    $email3 = ereg_replace(".", "#", "$email2");
    $email4 = ereg_replace("\n", "#", "$email3");
    $email4 = ereg_replace(" ", "#", "$email4");
    $email4 = ereg_replace("<", "#", "$email4");
    $email4 = ereg_replace(">", "#", "$email4");
    $email4 = ereg_replace("Content-Type", "#", "$email4");
    $email4 = strip_tags($email4);
}
```

```

// kijk na of de opgegeven domeinnaam wel bestaat
$emailrij = explode("@", $email);
$email5 = gethostbyname($emailrij["1"]);
$email5 = ereg_replace("\.", "", $email5);
$email5 = is_numeric($email5);
if ($email == $email2 || $email == $email3 || $email <> $email4
    || !$email5) {
    // er werden ongeldige karakters ingevoerd
    $fout .= "\n <li>Er werd geen geldig e-mailadres ingevoerd.</li>";
}
}

if ($fout <> "") {
    // er werden ongeldige dingen ingevoerd: weiger verder te gaan
    echo("\n<h2>Foutje</h2>");
    echo("\n");
    echo("\n<p>De ingevoerde gegevens waren niet correct. Bijgevolg kon
        het formulier niet verzonden worden. Meer bepaald:</p>");
    echo("\n");
    echo("\n<ul>");
    echo("$fout");
    echo("\n</ul>");
} else {
    // alles ok, je kan het formulier verder verwerken
}

?>

```

Doe een gelijkaardige controle op alle velden die je gebruikt om een mailtje te sturen via je contactformulier.

Hou mailinglijsten up-to-date

Maak je gebruik van mailinglijsten? Zorg dan dat de e-mailadressen in deze lijsten up-to-date zijn. Lijsten met verschillende verouderde of onbestaande adressen worden door de grote e-mailleveranciers als frauduleus beschouwt, waardoor je bij hen op een blacklist kan terechtkomen.

Een fictief maar concreet voorbeeld: je stuurt een mailtje naar lijst@mijngroep.be. In die lijst zitten 4 onbestaande *@yahoo.com*-adressen. Wanneer het mailtje aankomt op de servers van Yahoo, wordt deze fout door hen vastgesteld. Yahoo denkt *"hier zitten een paar spammers die proberen naar om het even welk Yahoo-adres mailtjes te sturen"* en zet *mijngroep.be* (of erger nog: het IP-adres van de hele Scoutnet-server) op de blacklist. Vanaf dan is het onmogelijk om vanaf de Scoutnet-server nog mailtjes te sturen naar de Yahoo-server, ook al gaat het deze keer misschien om bestaande mailadressen.

Let op met wachtwoorden

Veel mensen onderschatten het belang van wachtwoorden. Nochtans zijn ze even belangrijk als een goed slot op je huisdeur. Je laat toch ook niet de autosleutels op het contact van je wagen staan terwijl je even gaat winkelen?

Een degelijk wachtwoord helpt in de bestrijding van spam. Daarom een paar tips...

1. Kies een goed wachtwoord. Dat betekent: een combinatie van kleine en hoofdletters, cijfers en speciale karakters. Een kort wachtwoord is vanzelfsprekend minder betrouwbaar als eentje met 12 karakters. Voor belangrijke wachtwoorden kies je beter een *passphrase*. Een voorbeeld zou

kunnen zijn: *W@yS1wUg*. Dat staat voor *what you see is what you get*. Een passphrase is makkelijk te onthouden als je het zinnetje kent, en is vaak moeilijker te kraken.

2. Gebruik voor elke toepassing een apart wachtwoord. Het is zeker geen goed idee om voor je FTP-account hetzelfde wachtwoord te gebruiken als voor je MySQL-database.
3. Verander regelmatig je wachtwoorden. Hou eventueel voor jezelf bij op welke plaatsen je een wachtwoord nodig hebt. Voor een MySQL-verbinding zet je de nodige gegevens best in één bestand dat je dan op alle PHP-pagina's oproept. Eventueel kan je het bestand ook buiten de *public_html*-map zetten: daar staat het extra veilig.
4. Schrijf je wachtwoorden niet op en geef ze niet zomaar door via e-mail, ook niet aan Scoutnet zelf. Je kan het gratis programma BIC Note gebruiken om je lijstje met wachtwoorden op te slaan in een geëncrypteerd bestand. Zie <http://users.telenet.be/d.rijmenants/nl/bicnote.htm>.

TIPS VOOR INTERNETGEBRUIKERS

Laat niet overal je mailadres achter

Het is evident, en toch lopen nog elke dag mensen in deze val. Denk goed na vooraleer een e-mailadres op te geven, zeker op websites die je niet kent. Is het invoeren van een mailadres verplicht (bijvoorbeeld bij het schrijven van een berichtje in een gastenboek of bij de registratie op een site), overweeg dan welk adres je opgeeft.

Het is ook verstandig om een tweede mailadres te hebben dat je alleen voor zo'n doeleinden gebruikt. Als achteraf blijkt dat de makers van een website je spamberichten versturen, dan komen ze in deze testmailbox terecht en niet op je "serieuze" adres.

Voeg veilige domeinnamen toe aan je veilige lijst

De meeste mailleveranciers bieden je de mogelijkheid om te werken met veilige lijsten. Daar kan je mailadressen of zelfs volledige domeinnamen aan toevoegen. Op die manier voorkom je dat mails van je favoriete website in je spambox terecht komen.

Negeer ongevraagde reclame

Komt er toch ongewenste post in je mailbox? Verplaats ze dan naar je spambox (deze leren hieruit beter spam te detecteren voor toekomstige berichten) en/of verwijder de berichten. Het slechtste wat je kan doen, is klikken op de *subscribe-unsubscribe*-links (tenzij het om een website gaat waar je je wel degelijk ooit hebt op ingeschreven).

Waarom? Omdat klikken op deze links aan de afzender bevestigen dat jouw mailadres correct is en nog gebruikt wordt. Voor de spammers een goeie reden om ook in de toekomst naar dat e-mailadres spamberichten te sturen.

Let op voor phishing

Phishing is een door hackers gebruikte techniek om aan je wachtwoorden te geraken. Deze hackers sturen je in dat geval een mail waarin ze zich voordoen als jouw bank. Met een smoesje lokken ze je naar een website die visueel ook amper verschilt van deze van

je echte bank. Daar vragen ze om je wachtwoord of de code van je bankkaart in te voeren. En zonder het zelf te beseffen, hebben ze alle gegevens om je bankrekening te plunderen.

Onthoud daarom het volgende: geef nooit bankgegevens of wachtwoorden door aan onbeveiligde websites (websites die gebruik maken van een beveiligde lijn beginnen met <https://> in plaats van <http://>). Banken gaan nooit via een e-mail vragen om deze gegevens door te geven; ga er dan ook niet op in. Telefoon even naar je bank als je twijfelt over wat je moet doen.

Gelukkig zijn de nieuwste generatie browsers (zoals Internet Explorer 7 en Firefox 2) uitgerust met tools om deze vorm van criminaliteit te blokkeren. Maar wees op je hoede. Een gewaarschuwd man is er twee waard...

TOT SLOT

Dit lijstje mag dan behoorlijk lang zijn, het is zeker niet volledig. Heb je zelf nog een tips? Aarzel dan niet en bezorg ze ons per mail naar info@scoutnet.be. Misschien vond je de uitleg hierboven soms te technisch of heb je bijkomende vragen? Via ons forum op <http://forum.scoutnet.be> helpen we je graag verder.

... want alles kan beter! ;o)

Thomas Rumbaut
Scoutnet Team
Oktober 2006