



June Newsletter: Don't get hooked – 3 ways to spot a phish

Hello!

Hackers are savvy. A few years ago, the most sophisticated email scams involved Nigerian princes asking you to send money in return for a payout. As the public has become more Internet savvy, hackers have developed schemes that are harder to detect.

At Cartwheel, we often receive calls about fraudulent links and emails scams. In this month's newsletter we'll discuss phishing, and give you a few tech-savvy ways to detect whether an email is a fake.

All the best,

Josh Feder
Co-founders

What is a phishing email?

Phishing emails are emails that seek to collect your personal information by posing as a trustworthy entity such as a bank or well known company. The emails direct you to a fake web site or ask you to call a phone number, at which point they will collect your personal data. The emails are tailored to look authentic, which makes them difficult to distinguish from the real thing.

How to Spot a Phish:

Although Phishers are savvy, below are 3 ways to tell your e-mail is a phishing scheme. Please note, the absence of these does not mean your e-mail is safe.

1. Check the Links

Phishing e-mails that make it to your inbox have links that you can click on. In most e-mail programs, rolling over the link will reveal the web address that the link will send you to. If the link is not exactly the same as the real entity, you know its spam.

Below is a Phishing e-mail pretending to be from Facebook. Notice that the link sends me to an unrelated web site.



From: Facebook [mailto:update+hwtvsuwj@facebookmail.com]
Sent: Saturday, June 12, 2010 11:31 AM
To: partners
Subject: Angelina Jolie invited you to join Facebook...

A screenshot of an email from Facebook. The email header is in a blue bar with the word "facebook" in white. The main body of the email is white. It starts with "Hi," followed by "The following person invited you to be their friend on Facebook:". Below this is a link to "Angelina Jolie" and a smaller link to "http://technoline.ca/z.htm". To the right of the main text is a yellow box with the text "Facebook is free and anyone can join." and a green "Sign Up" button. At the bottom of the email, there is a yellow box with the text "To sign up for Facebook, follow the link below:". The email also includes a "Thanks, The Facebook Team" and a link to "Already have an account? Add this email address to your account here.".

facebook

Hi,

The following person invited you to be their friend on Facebook:

[Angelina Jolie](#)
Invite
Set 1
2010 21:00:51
+0530

<http://technoline.ca/z.htm>

Facebook is free and anyone can join.

Sign Up

Facebook is a great place to keep in touch with friends, post photos, videos and create events. But first you need to join! Sign up today to create a profile and connect with the people you know.

Thanks,
The Facebook Team

Already have an account? Add this email address to your account [here](#).

To sign up for Facebook, follow the link below:

2. Check the Sender

Most e-mail programs show both the name of the sender, as well as the e-mail address from which it came. When the e-mail address is unrelated to



the name of the sender, it's a tip-off that the e-mail is a fake. In the Facebook phishing e-mail above, you can see that the send name is "Facebook", but the e-mail address is "update+hwtvsuwjatfacebookmaildotcom", obviously a fake.

3. Check the Internet Header

Every e-mail has a "postmark" attached to it. This postmark, called an internet header, contains information about where the e-mail came from, and how it got to you.

To see an internet header in Outlook, simply right-click on an e-mail and select "Message Options.". Below is part of the header from the fake Facebook email. Notice the Reply-To address, which is clearly unrelated to Facebook.

```
Received: from exmf018-1.msoutlookonlinedotnet
(10.254.253.34) by EXHUB018-
4.exch018.msoutlookonlinedotnet (64.78.17.44) with Microsoft
SMTP Server id 8.2.234.1; Sat, 12 Jun 2010 08:31:52 -
0700 Date: Sat, 12 Jun 2010 21:00:51 +0530 From:
Facebook update+hwtvsuwjatfacebookmaildotcom X-Mailer:
The Bat! (v3.80.03) Professional Reply-To:
shittyz442atrealexcellencedotcom X-Priority: 3
(Normal) Message-ID:
904947535.73427578249891atrealexcellencedotcom To:
partners@ptsolutionsdotcom Subject: Angelina Jolie invited you
to join Facebook... MIME-Version: 1.0
```

Some parting words about avoiding phishing scams: You often read advice about using junk-mail filters, phishing filters, etc. While all those are useful, the secret to avoiding phishing is simple.

Never, ever, ever, enter or give any SOLICITED personal information. No real company would ask you for this information through an e-mail solicitation.