



## Staff briefing on Phishing

### Summary

If you are concerned about identity theft (as indeed you should be!), it is in your interests to find out about phishing. Phishing is a social engineering technique using emails and fake websites to lure victims into parting with personal information such as their credit card numbers. This briefing describes phishing and suggests how to minimize your risk of being caught.

### What is phishing and how does it work?

Phishing is a form of fraud, used to commit identity theft. The term “phishing” reflects the way that fraudsters trawl and lure their victims through the net, rather like fishermen at sea.

Phishing emails look as if they are from organizations such as your bank, credit card company or PayPal (see below for examples). They typically ask you to click a link to “update” or “verify” or “confirm” certain information. If you click the link to visit the website, the site looks like the company’s website but it is really a fake controlled by the phishers. Any information you enter is captured by them and may be used for identity theft. Some even display the authentic padlock symbol – this simply means your personal details are encrypted whilst being sent to the phishers!

Some phishers trick Internet Explorer and other browsers into concealing the real address of their fake website. Tricks include using very long URLs (often containing lots of % characters making them hard for users to understand) and exploiting various software bugs. **Sometimes, simply visiting a fake phisher or hacker website can be enough to compromise your system** – you may not even have to enter your data into the phisher’s form. Thankfully, such attacks are quite rare but they are a very good reason to keep your computer up-to-date with security patches.

### How to recognize phishing emails

There are usually clues in phishing emails that betray them as possible fakes. Often, they:

- Are unsolicited – they arrive out of the blue (even if you are expecting to hear from your bank, be very wary if an email arrives asking for personal information. No responsible bank would ask for this kind of information in an email).
- Use authentic-looking logos *etc.* that are simply copied from the real company’s website.
- Tell you to respond urgently to avoid something bad. Stop and think! Having your identity stolen is much worse than having your PayPal account suspended or whatever.
- Contain spelling or grammatical errors.
- Tell you to click on a link and ‘update’, ‘confirm’ or ‘verify’ your information (sometimes phishing emails include a data-entry form rather than a link to a website).
- Look formal, typically with some officious or legal mumbo-jumbo.
- Address you in vague terms instead of by your full name, and don’t give account IDs or other identification information except for your email address.
- Warn you not to reply to the message *e.g.* “because the email address is not monitored” (but be aware that some legitimate emails also say this!).

Take a look at the example phishing emails below to see the clues in the messages.

## AOL phishing email

If I was naïve enough to think I could get a free AOL account and had not been quite so alert, I might have clicked on “Click here to get your own AOL account for free”:

**From:** Admin [sender's EMAIL address was here, probably spoofed]  
**Sent:** 22 September 2003 21:29  
**To:** [Recipient EMAIL address was here]  
**Subject:** AOL totally without charge

The free ISP (Internet service provider) is one of those ideas whose time has come but whose reality has yet to catch up. It's been one of the recurring stories over the last year and a half, not only because of the growing number of companies offering free, ad-supported Internet access, but because of its impact, both real and potential, on some of the Internet's most established businesses.

SO as time changes so does AOL . SO for the first time in history AOL is now FREE !!! that's right all you need is a computer and a internet connection to receive all AOL has to offer for FREE...

[Click here to get you're own AOL account for free](#)

please note this this invitation will never be sent again so please take this opportunity...thank you for you're time sincerely you're friends at [www.AOL.com](http://www.AOL.com)

The [www.AOL.com](http://www.AOL.com) link at the bottom really did link to AOL's website. However the free AOL account link went to a server with a numeric IP address. Notice the spelling mistakes and grammatical errors (e.g. “you're own” should be “your own”).

## PayPal phishing email

What looked like a legitimate PayPal link on the screen (<https://www.paypal.com...>) was in fact a hyperlink to a fake PayPal-lookalike web site controlled by the phishers. There, I was encouraged to enter my personal information but if I had done so, it would have gone directly to the fraudsters not to PayPal. Notice the authentic-looking PayPal logo and colors.



Dear PayPal member,

At PayPal, we value the trust you have placed in us by using our service to conduct your transactions online. Because our relationship with you is financial in nature, the protection of your privacy is particularly important to us.

We are sending this verification notice to provide you with information about how PayPal safeguards your privacy, as well as to comply with U.S. federal privacy guidelines that apply to financial institutions such as PayPal. The full terms of PayPal's privacy policy are available on the PayPal website, which you are welcome to review at any time.

**Please verify your account and financial information by clicking on the link below:**

<https://www.paypal.com/cgi-bin/webscr?cmd=verify>

\*\*\* DO NOT REPLY TO THIS EMAIL \*\*\*

Copyright© 2003 PayPal, Inc. All rights reserved. Designated trademarks and brands are the property of their respective owners.

Compare the fake above with a genuine email from PayPal shown on the next page ...

**A genuine PayPal email (for comparison)**

From: service@paypal.co.uk [<mailto:service@paypal.co.uk>]

Sent: 29 July 2005 04:35

To: <My email address was here>

Subject: Credit Card Expiry Date Approaching

Dear <My name was here>,

Your credit card ending in <The last 4 digits were here> will expire soon.

To avoid any interruption to your service, please update your credit card expiry date by following the steps below. If you do not update your credit card expiry date

- You will no longer be able to fund payments with this card

To update your credit card expiry date:

1. Log in to your PayPal account
2. Go to the Profile subtab
3. Click on the 'Credit Cards' link in the Financial Information column
4. Select the radio button next to the credit card you would like to update and click 'Edit'
5. Enter your credit card verification number
6. Enter the new credit card expiry date
7. Click 'Save'

Thank you for using PayPal!

The PayPal Team

-----  
**PROTECT YOUR PASSWORD**

NEVER give your password to anyone, including PayPal employees. Protect yourself against fraudulent websites by opening a new web browser (e.g. Internet Explorer or Netscape) and typing in the PayPal URL every time you log in to your account.

-----  
Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For assistance, log in to your PayPal account and click the Help link located in the top right corner of any PayPal page.

-----  
PayPal (Europe) Limited is authorised and regulated by the Financial Services Authority in the United Kingdom as an electronic money institution.

PayPal Email ID PP031

**Here are some clues to its authenticity:**

- The credit card referenced really was due to expire in a few days, so this email was not unexpected (big clue!).
- It was addressed to the account holder by name, not "PayPal customer" etc.
- It included part of a real credit card number, something phishers (hopefully!) would not know.
- There was a brief warning about exactly what would happen if the card expired - no hyperbole about terrible things, no implied threats about being prosecuted as a fraudster or whatever.
- It told the recipient to visit the PayPal site, login and make the changes, but had no (zero, not one, count them) hyperlinks in the message.
- It was well written, without spelling mistakes and grammatical errors.
- It was a plain text message without impressive-looking but easily-faked PayPal logos etc.

## How to avoid being caught by the phishers

### 1. Things you can do

- Keep your home systems updated with security patches (corporate systems are patched automatically by IT department – please do not interfere with or try to patch corporate systems);
- Don't take emails or websites at face value. Be on your guard!
- Be extremely wary of any unsolicited request for your personal information, especially if financial or other sensitive information (such as your password or Social Security Number) is requested.
- The most prevalent form of phishing involves emails at present but fraudsters could use the telephone or possibly even face-to-face contact to get your personal details.
- Verify any request for personal information before you respond e.g. telephone the bank, credit card company or other (apparent) sender using the standard switchboard or customer services number (phone numbers or email addresses stated in the email may be fakes!).
- Report suspicious emails to Information Security Management and/or the authorities e.g. the Federal Trade Commission, the Police *etc.*

### 2. Things that companies are doing

PayPal is an excellent example of a company taking proactive steps to foil the phishers:

- Their website advises visitors on how to spot fake emails, and makes some solid commitments e.g. they will always refer to their customers by name in emails, and will never request sensitive information by email.
- They publish an email address ([spoofoff@paypal.com](mailto:spoofoff@paypal.com)) for users to notify them of suspicious emails, giving them a fighting chance of tracing and hopefully stopping these frauds before their customers lose out.
- They actively search for phisher websites and, wherever possible, get them closed down quickly (this is not easy to do in some parts of the world).
- They monitor their own email accounts (including Hotmail and other accounts set up just to lure phishers) for phishing emails.
- They are notified about possible phishers by responsible customers and by industry bodies set up to share information on phishing (e.g. [www.AntiPhishing.org](http://www.AntiPhishing.org)).
- Behind the scenes, PayPal's employees are trained to analyze and respond appropriately to potential phisher emails. They have cooperative working relationships with law enforcement and other official bodies such as the Federal Trade Commission, and with their industry peers. They keep a close watch on hacker websites and newsgroups for intelligence about phisher techniques, especially anyone who mentions eBay or PayPal.

## Conclusion

Phishing is a growth industry. Being aware of this problem and taking the steps explained in this briefing will significantly reduce the chance of you being caught in the phishers' net.

## For more information

For information on phishing and identity theft, talk to Information Security or visit Information Security's intranet website for links to useful Internet websites. **If you think you might have been caught by a phisher, call the IT Help Desk and your bank as soon as possible for further advice.** Acting quickly may help protect your identity.