

E Services for Business



Email / Mail Boxes

Pop mail scanned for virus before delivery to you. As close to 100% virus removal as possible. WebMail facility so you can read and send email out of office.

SMTP Backup Mail Server

Peace of mind knowing that if your mail server is offline for any reason ours will collect and hold all your mail for you until you are ready to receive it.

SMTP Plus Mail Service

All mail scanned for virus and removed. Enhanced spam filters with settings you can tweak until completely happy.

Local AntiVirus Protection

Stay safe with NOD 32—award winning, advanced heuristic antivirus detection and removal software.

Business Quality ADSL / Broadband

Fast and reliable business broadband to make sure you stay connected. Comes with 5 free mail boxes or free SMTP backup mail service as above.

Standard Dialup Internet Access

Not everyone needs or wants Broadband. If this is you we can offer a dialup internet connection with free mail box (as above).

Web Sites & Hosting

A home for your web site on some of the fastest, best connected web servers in the UK. Includes WebBuilder—the easy way to make your own web site. Safe and secure from burglars and hackers too.

Dedicated Server Hosting

Rent or buy and then place with us at the excellent Telehouse facility in Docklands, London. THE "place to be" on the Internet.

Domain Name Registration

We can register your domain name and then look after it for you. We run our own Name Servers and you are guaranteed a fast and competent service.

Friendly and Professional Experts

You don't need to know everything about the Internet because we know it for you. Help when you need it, at local call rates.

Netpresto is a privately owned limited company Registration number 3663411. It was established in 1998 by Steve Newcombe MBCS, who has spent his whole career in the IT Industry, to provide technical Internet Services to SMEs. Our sister company PCS Professional Computer Services, established in 1986, is housed in the same premises and provides IT Security Services.

Our mission critical web, mail and domain name servers and routing equipment are located in a power resilient, safe, physically secure environment—TheTelehouse Data Centre in Docklands London. Telehouse has connections to the Internet backbone that are second to none. All our equipment is remotely monitored and managed 24 hours a day.

Our office is located in the Bridges Conservation Area of Gateshead, a few minutes walk from the Sage and the Baltic. We are at the Gateshead end of the High Level Bridge.

Connecting your business is our business

9-11 Wellington Street
Gateshead
NE8 2AJ

Phone: 0845 003 88 88
Fax: 0845 003 88 89

Netpresto Ltd 0845 003 88 88

www.netpresto.co.uk

Netpresto Ltd 0845 003 88 88

Phishing—What it is and how to avoid getting caught



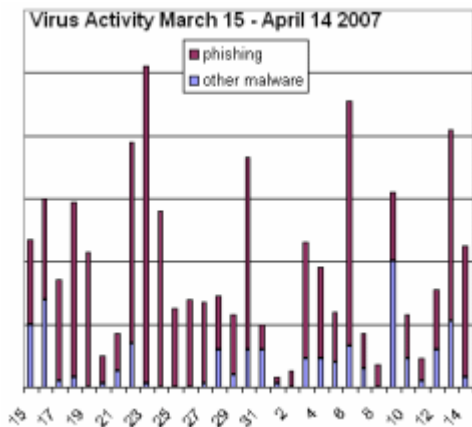
What is phishing?

A phishing email is jargon for a type of email designed to trick you in to parting with valuable personal information—usually related to your financial accounts.

The emails often impersonate banks, credit card companies, Ebay and Paypal. What they hope to achieve is that you visit a fake web site and enter your login and password. Your details are recorded and then used in fraudulent transactions.

How big is the threat?

This graph extracted from our mail server statistics for March/April shows that Phishing continues to be a major hazard for email users. The Phishing emails (red) far outnumber other malware (blue).

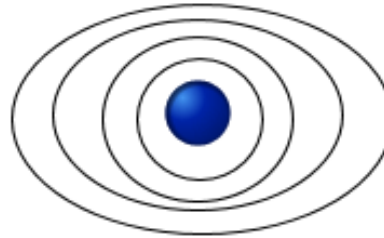


How do we protect you?

For customers whose mail travels through our systems—pop mail and 'SmtP Plus' mail users—there are several rings of defence in place:- mail server challenging, firewalls, inbound mail analysis and processing, scanning and malware removal, and—very importantly—regular monitoring by us.

If however you receive your mail directly with your own mail server and smtp mail, then you should have all these defences in place yourself.

This year we have stopped many thousands of these emails reaching our customer's mail boxes. However, in common with all other ISPs, we cannot guarantee that every phishing email will be caught because new variants appear frequently.

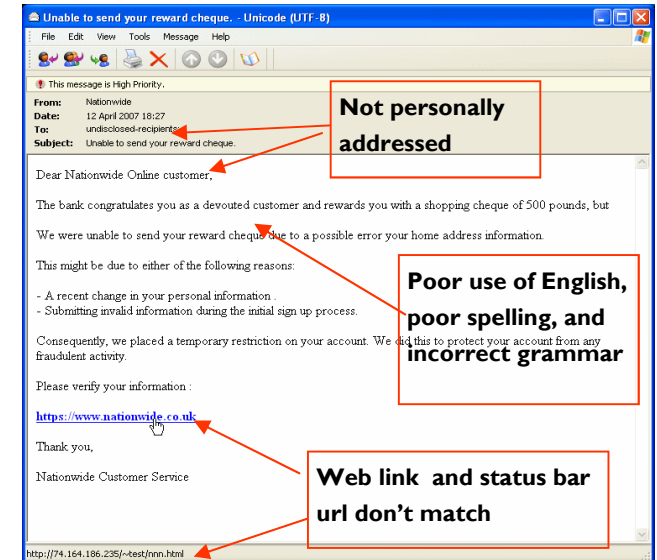


How can you protect yourself?

There are two main areas to consider. The first is to run an up to date local antivirus software with a heuristic engine—one that is capable of learning such as NOD32. The second is to be armed with information and examine any suspicious emails carefully:-

- Was the email sent to you personally?
- Is the greeting generic or missing?
- If the email contains a clickable web link does it match the url displayed in the status bar when you move your mouse over the link?
- Most banks use a secure site for account access. Check that login links go to a secure web site (https://).
- Is the spelling correct and grammar good?
- Are the company details shown, are they correct and is any copyright information current?
- Is the domain registered to the business?
- Be wary of similar looking domain names e.g paypai.com instead of paypal.com

Below is an example of a recent phishing email campaign. This is a fairly crude attempt and has a number of suspicious elements. However care should be taken—some emails and fake sites are quite sophisticated.



Always be wary of emails that ask you to login to any account by clicking a link they contain.

If you think the email may be genuine and you want to login to your account do not click the link—instead open a new web browser window and type in the usual web address you use for that organisation.

Stay up to date on current threats. Visit your bank's web site or Bank Safe Online for up to date information and advice.
<http://www.banksafeonline.org.uk/>
If you think you have fallen victim contact your bank immediately and change your password.