How to be safe from phishing?

What is phishing?

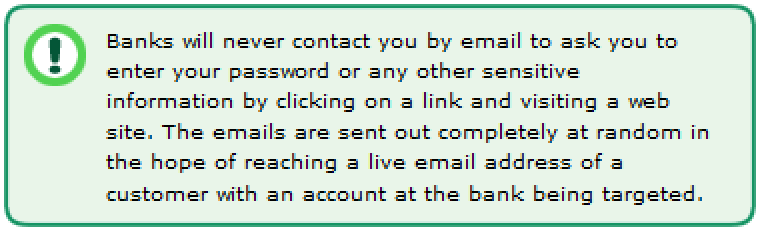
Phishing is a fraudulent attempt, usually made through email, to steal your personal information. The best way to protect yourself from phishing is to learn how to recognize a phish.

Phishing emails usually appear to come from a well-known organization and ask for your personal information — such as credit card number, social security number, account number or password. Often times phishing attempts appear to come from sites, services and companies with which you do not even have an account.

In order for Internet criminals to successfully "phish" your personal information, they must get you to go from an email to a website. Phishing emails will almost always tell you to click a link that takes you to a site where your personal information is requested. Legitimate organizations would never request this information of you via email.

How can I prevent myself being a victim of phishing?

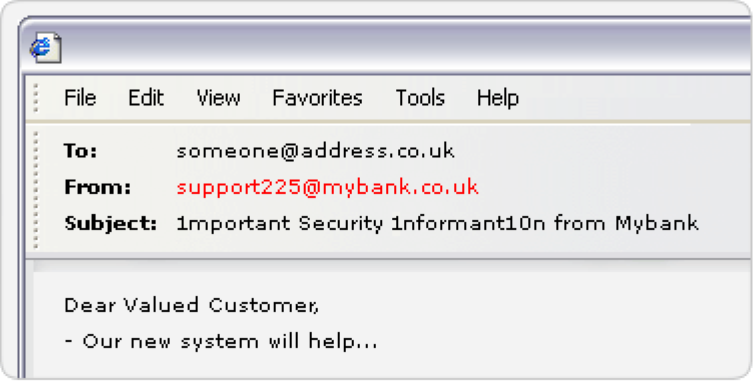
The key thing is to be suspicious of all unsolicited or unexpected emails you receive, even if they appear to originate from a trusted source. Although your bank may contact you by email, they will never ask you to reconfirm your login or security password information by clicking on a link in an email and visiting a web site. Stop to think about how your bank normally communicates with you and never disclose your password in full or personal information.



Banks will never contact you by email to ask you to enter your password or any other sensitive information by clicking on a link and visiting a web site. The emails are sent out completely at random in the hope of reaching a live email address of a customer with an account at the bank being targeted.

How to spot a phishing email

1 - Who is the email from?



To: someone@address.co.uk
From: support225@mybank.co.uk
Subject: 1mportant Security 1nformant10n from Mybank

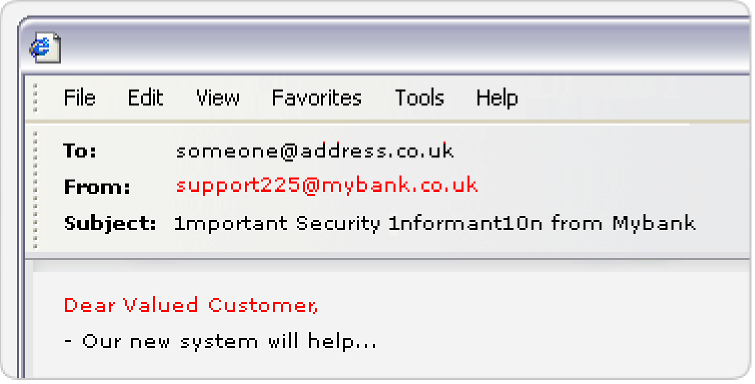
Dear Valued Customer,
- Our new system will help...

Phishing emails can look like they come from a real bank email address. Unfortunately the way Internet email works makes it a relatively simple matter for phishers to create a fake entry in the "From:" box.

The email address that appears in the "From" field of an email is NOT a guarantee that it came from the person or organisation that it says it did. These emails were not send using the bank's own systems.

2 - Who is the email for?

The emails are sent out at random to bulk email lists and the fraudsters will almost certainly not know your real name or indeed anything else about you, and will address you in vague terms like "Dear Valued Customer".



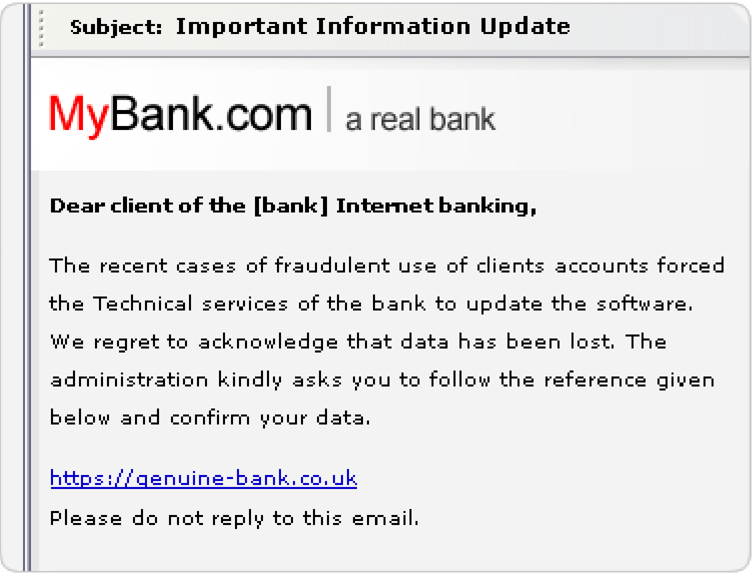
To: someone@address.co.uk
From: support225@mybank.co.uk
Subject: 1mportant Security 1nformant10n from Mybank

Dear Valued Customer,
- Our new system will help...

3 - Take a closer look at the email - does it look "phishy"?

The first thing to remember is that banks will never write to you and ask you for your password or any other sensitive information by email. The message is also likely to contain odd "spe11ings" or cApitALs in the "Subject:" box (this is an attempt to get around spam filter software), as well as grammatical and spelling errors.

Example scam email:



Subject: Important Information Update

Dear client of the [bank] Internet banking,

The recent cases of fraudulent use of clients accounts forced the Technical services of the bank to update the software. We regret to acknowledge that data has been lost. The administration kindly asks you to follow the reference given below and confirm your data.

https://genuine-bank.co.uk

Please do not reply to this email.

Never log-on to your online banking account by clicking on a link in an email. Open your web browser and type the bank's address in yourself.

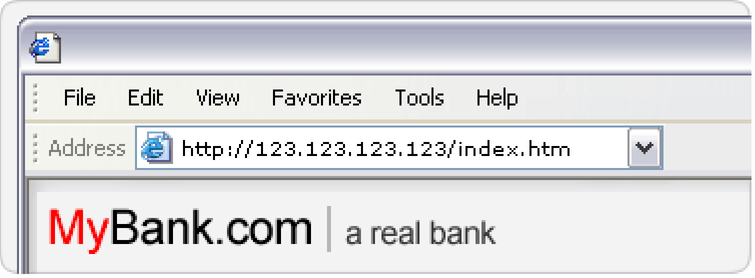
If in any doubt about the validity of an email purporting to come from your bank, contact them on an advertised phone number.

4 - Where's that hyperlink going to?

Unfortunately it is all too possible to disguise a link's real destination, so the displayed link and anything which shows up in the status bar of your email programme can easily be falsified.

How to spot a Phishing web site

What's the site address?



http://123.123.123.123/index.htm

If you visit a web site after clicking on a link from an email, there are many ways of disguising the true location of a fake web site in the address bar. The site address may start with the genuine site's domain name, but that is no guarantee that it points to the real site. Other tricks include using numerical addresses, registering a similar address (such as www.mybank-verify.com), or even inserting a false address bar into the browser window. Many of the links from these pages may actually go to the genuine web site, but don't be fooled.

Beware of fraudulent pop-up windows

Instead of displaying a completely fake web site, the fraudsters may load the genuine web site in the main browser window and then place their own fake pop-up window over the top of it. Displayed like this, you can see the address bar of the real web site in the background, although any information you type into the pop-up window will be collected by the fraudsters for their own usage.

To access your online banking account, type the address into a new window yourself. The address of your genuine bank site will start https and will include a small padlock in the bottom of the browser window.

Reference

http://www.banksafeonline.org.uk/phishing_explained.html