PJC accounting services

☎ 01929 550 802
✉ office@pjcacs.co.uk

FACT FILE

8 Ways To Avoid Phishing Scams

1. Guard against spam. Be especially cautious of emails that:

* Come from unrecognized senders.

* Ask you to confirm personal or financial information over the Internet and/or make urgent requests for this information.

* Aren't personalized.

* Try to upset you into acting quickly by threatening you with frightening information.

2. Communicate personal information only via phone or secure web sites. In fact:

When conducting online transactions, look for a sign that the site is secure such as a lock icon on the browser's status bar or a "https:" URL whereby the "s" stands for "secure" rather than a "http:".

Also, beware of phone phishing schemes. **Do not divulge personal information over the phone unless you initiate the call**. Be cautious of emails that ask you to call a phone number to update your account information as well.

3. Do not click on links, download files or open attachments in emails from unknown senders. It is best to open attachments only when you are expecting them and know what they contain, even if you know the sender.

4. Never email personal or financial information, even if you are close with the recipient. You never know who may gain access to your email account, or to the person's account to whom you are emailing.

5. Beware of links in emails that ask for personal information, even if the email appears to come from an enterprise you do business with. Phishing web sites often copy the entire look of a legitimate web site, making it appear authentic. To be safe, call the legitimate enterprise first to see if they really sent that email to you. After all, businesses should not request personal information to be sent via email.

6. Beware of pop-ups and follow these tips:

* **Never enter personal information in a pop-up screen**.

* Do not click on links in a pop-up screen.

* Do not copy web addresses into your browser from pop-ups.

* Legitimate enterprises should never ask you to submit personal information in pop-up screens, so don't do it.

7. Protect your computer with a firewall, spam filters, anti-virus and anti-spyware software. Do some research to ensure you are getting the most up-to-date software, and update them all regularly to ensure that you are blocking out new viruses and spyware.

8. Check your online accounts and bank statements regularly to ensure that no unauthorized transactions have been made.

You should **always be careful about giving out personal information over the Internet**. Luckily, companies have begun to employ tactics to fight against phishers, but they cannot fully protect you on their own.

Remember that you may be targeted almost anywhere online, so always keep an eye out for those "phishy" schemes and **never feel pressure to give up personal information online**.

Information from www.identitytheftkiller.com