Withdrawn

This publication is withdrawn.

This publication is no longer current.

Department for Work & Pensions

Advice about online security

May 2013

Contents

Report a suspicious email or website 3

Security advice 5

Genuine DWP contacts 8

Recognising and reporting phishing and bogus emails 9

How DWP keeps you safe online 12

Useful external links 14

Report a suspicious email or website

DWP will never ask you by email to disclose personal or payment information, reset security settings or authenticate login and payment details. If you have any doubt that an email you receive from DWP is genuine please do not follow any links, disclose any personal details or respond to it. Please forward it to the following email address and then delete it.

DWP.PHISHING@DWP.GSI.GOV.UK

Phishing is emailing someone to fraudulently to get their personal or financial information such as passwords, credit card or bank account details.

If you are suspicious of an email you have received about your benefit or Department for Work and Pensions (DWP) services, please forward it to the following email address and then delete it.

DWP.PHISHING@DWP.GSI.GOV.UK

Bogus web pages are counterfeit or fake web pages that make people believe they are on the genuine web site, that is they are designed to look like or similar to a bank, DWP or GOV.UK website.

If you think that a website may be bogus and it relates to DWP or GOV.UK, please forward the web address for it to the following email address.

DWP.PHISHING@DWP.GSI.GOV.UK

What you should do if you have disclosed personal details

DWP will never ask you by email to disclose personal or payment information, reset security settings or authenticate login and payment details. If you have any doubt that an email you receive from DWP is genuine please do not follow any links, disclose any personal details or respond to it. Please forward it to the following email address and then delete it.

DWP.PHISHING@DWP.GSI.GOV.UK

However, if you have already given any of your personal information, for example your password or National Insurance number, in reply to a suspect email please forward the original email (not any reply that may include your personal information), a brief description of what has happened and a telephone contact number, to the email address below:

DWP.PHISHING@DWP.GSI.GOV.UK

Please **do not** disclose any of your personal details or information in your email report to DWP. It would help any investigation if you could tell us the type(s) of information that you gave to the suspect website. For example – I gave my name, address, date of birth, bank account details etc.

Security advice

DWP will never ask you by email to disclose personal or payment information, reset security settings or authenticate login and payment details. If you have any doubt that an email you receive from DWP is genuine please do not follow any links, disclose any personal details or respond to it. Please forward it to the following email address and then delete it.

DWP.PHISHING@DWP.GSI.GOV.UK

Making your online experience as secure as possible

Electronic communication and transactions are a key part of DWP business but there is always the risk of fraud – people claiming to be someone they are not and getting information they should not have

DWP, in common with all providers of online services, is committed to your security – but you need to be alert.

DWP continuously monitor systems and customer records to guard against fraudulent activity. The methods fraudsters use to obtain the information they want is constantly changing, so DWP will provide updates on this website on the type of scams it is aware of. The main risk involves the stealing of identity or access details.

Please do everything you can to ensure that the identifiers and passwords you use when using DWP systems are kept secure and updated regularly. You should not give your online User ID and password to anyone. Any suspicious activity should be reported to DWP immediately.

How to protect yourself online

Password and login details

Keep your password and login details secure, and make sure they are changed regularly. Do not write them down or tell anyone what they are, including DWP staff.

Unsolicited emails

Be suspicious of emails from people or companies that you don’t know, even if they look like they're from a trusted source.

DWP will never ask you by email to disclose personal or payment information, reset security settings or authenticate login and payment details. If you have any doubt that an email you receive from DWP is genuine please do not follow any

links, disclose any personal details or respond to it. Please forward it to the following email address and then delete it.

DWP.PHISHING@DWP.GSI.GOV.UK

Do not include any further personal information and once you have sent it please delete it.

Please be aware that DWP are unable to investigate paper copies of phishing emails and websites. In order for DWP to take any action, you will need to forward the original phishing email to the email address provided.

Anti-virus software

Make sure your computer has anti-virus and anti-spyware software, and that it is continually updated to the latest version.

Personal firewall and secure wireless network

Make sure any computer which connects to the internet has appropriate firewall protection to block any unauthorised connections being made. If you're using a wireless network, ensure it is secure.

Find out more about secure wireless networks

Update your web browser

Use the most up to date version of your preferred web browser, this could reduce your chance of falling victim to online phishing scams, by displaying messages to alert you.

Keep your operating system up to date

Make sure you download and install updates regularly.

Sensitive information

Never enter sensitive information such as account details, PINs or passwords via a website link within an email.

Secure websites

Ensure websites are secure – look for the prefix 'https' in the address bar and a locked padlock or unbroken key symbol on the screen. Check the authenticity of a secure website by double clicking on the symbol. If you are in doubt contact the website owner on a phone number you have obtained yourself and not from the suspicious email.

Please see the section on ‘How DWP keep you safe online’ for further information about secure web pages.

The main risk involves the stealing of identity or bank details. Please do everything you can to ensure that the identifiers and passwords you use when accessing DWP systems are kept secure and updated regularly

Attachments and emails

Beware of attachments and emails – even if they appear innocent, they could contain a virus designed to steal your personal information.

Bogus websites

Type the full address of secure websites into your browser, rather than searching for it – this helps avoid being misdirected to a bogus site.

Websites charging for services

Please be aware that some websites offer services which DWP will provide at no cost. These include for example connection charges to DWP Telephone Helplines. Ensure you only contact DWP via addresses and numbers taken from GOV.UK or DWP.GOV.UK websites.

Genuine DWP contacts

DWP will never ask you by email to disclose personal or payment information, reset security settings or authenticate login and payment details. If you have any doubt that an email you receive from DWP is genuine please do not follow any links, disclose any personal details or respond to it. Please forward it to the following email address and then delete it.

DWP.PHISHING@DWP.GSI.GOV.UK

DWP is always looking for ways of improving communication with customers and this means they may occasionally contact you in new ways.

DWP know that you need to be able to confirm that any electronic contact you receive from them is genuine. If you want to contact DWP you should only use addresses and numbers obtained from either the GOV.UK or DWP.GOV.UK web pages.

Please be aware that some websites offer and charge for call connection services which DWP will provide without any additional charge. These include for example call forwarding services which include connection charges to DWP Telephone Helplines.

Ensure you only contact DWP via addresses and numbers taken from GOV.UK or DWP.GOV.UK websites.

Recognising and reporting phishing and bogus emails

DWP will never ask you by email to disclose personal or payment information, reset security settings or authenticate login and payment details. If you have any doubt that an email you receive from DWP is genuine please do not follow any links, disclose any personal details or respond to it. Please forward it to the following email address and then delete it.

DWP.PHISHING@DWP.GSI.GOV.UK

What is a phishing email?

Phishing is the fraudulent act of emailing a person in order to obtain their personal and financial information such as passwords, credit card or bank account details. These emails often include a link to a bogus website encouraging you to enter your personal details.

The guidance below may help you to recognise a phishing email.

Remember:

- DWP will never ask you to disclose personal or payment information by email
- to be completely safe from phishers, do not select links in emails. If in doubt, close your browser, reopen it, and type the web address for the site you want to visit directly into the address bar.

How to report DWP related phishing and bogus emails

If you have received a DWP related phishing and bogus email, please forward it to the following email address and then delete it.

DWP.PHISHING@DWP.GSI.GOV.UK

Hints and tips below may help you recognise a phishing or bogus email

Incorrect 'From' address

Look out for a sender's email address that is similar to, but not the same as, DWP's email addresses. Fraudsters often have email accounts with DWP or benefit names in them (such as 'benefits@dwp.org.uk'). These email addresses are used to mislead you.

However be aware, fraudsters can falsify (spoof) the 'from' address to look like a legitimate DWP address (for example '@dwp.gov.uk').

Personal information

DWP will never ask you to provide confidential or personal information such as passwords, credit card or bank account details by email.

Urgent action required

Fraudsters want you to act immediately. Be wary of emails containing phrases like 'you only have three days to reply' or 'urgent action required'.

Bogus websites

Fraudsters often include links to webpages that look like the homepage of a website. This is to trick you into disclosing personal or confidential information. Just because the page may look genuine, does not mean it is. Bogus webpages often contain links to banks and building societies, or display fields and boxes requesting your personal information such as passwords, credit card or bank account details.

You should be aware that fraudsters sometimes include genuine links to DWP webpages in their emails, this is to try and make their emails appear genuine.

Common greeting

Fraudsters often send high volumes of phishing emails in one go so even though they may have your email address, they don't often have your name. Be cautious of emails sent with a generic greeting such as 'Dear Customer'.

Look out for

Spelling mistakes and poor grammar.

Attachments

Be cautious of attachments as these could contain viruses designed to steal your personal information.

If you are suspicious of the email you have received, please forward it to the following email address and then delete it.

DWP.PHISHING@DWP.GSI.GOV.UK

What you should do if you have disclosed personal details

You should never disclose your personal or payment information in reply to an email that may look like it's from DWP, you may well be revealing your details to a fraudulent website.

However, if you have already given any of your personal information, for example your User ID, password or National Insurance number, in reply to a suspect email please forward the original email (not any reply that may include your personal

information), a brief description of what has happened and a telephone contact number to the email address below.

DWP.PHISHING@DWP.GSI.GOV.UK

Please **do not** disclose any of your personal details or information in the email report to DWP. It would aid any investigation if you could tell us the type(s) of information that you disclosed to the suspect website. For example – I gave my name, address, date of birth, bank account details etc.

DWP will act upon all DWP related phishing emails, removing reported fraudulent websites.

How DWP keeps you safe online

DWP will never ask you by email to disclose personal or payment information, reset security settings or authenticate login and payment details. If you have any doubt that an email you receive from DWP is genuine please do not follow any links, disclose any personal details or respond to it. Please forward it to the following email address and then delete it.

DWP.PHISHING@DWP.GSI.GOV.UK

DWP takes online security very seriously. Here are just some of the measures we take to protect you and your data.

Firewall protection

DWP use firewall protection as a very effective high security barrier around its systems and your data. This detects any attempts at unauthorised entry.

Security certificates

Any page of the DWP website which contains sensitive information is protected by a technology known as SSL (Secure Sockets Layer).

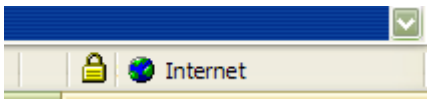
There are two general indications of a secured web page:

1) Check the web page URL (web page address)

Normally, when browsing the web, the URLs (web page addresses) begin with the letters "http". However, over a secure connection the address displayed should begin with "https" – note the "s" at the end.

2) Check for the "Lock" icon

There is a de facto standard among web browsers to display a "lock" icon somewhere in the window of the browser (**not** in the web page display area!) For example, Microsoft Internet Explorer displays the lock icon in the lower-right of the browser window:



As another example, Mozilla's FireFox Web Browser displays the lock icon in the lower-left corner:

The lock icon is not just a picture!

Click (or double-click) on it to see details of the site's security. This is important to know because some fraudulent web sites are built with a bar at the bottom of the web page to imitate the lock icon of your browser! Therefore it is necessary to test the functionality built into this lock icon.

Useful external links

You may find these links useful, however they are not under DWP control and it is not responsible for their content.

- Get safe online (Opens new window)
- Bank safe online (Opens new window)
- UK Payments Administration (Opens new window)