National Cyber Security Centre
a part of GCHQ

Phishing: guidance for political parties and their staff

This guidance has been produced for individuals and IT departments within political parties ahead of the forthcoming general election. It provides advice on how to detect phishing attacks and suggests preventative measures that should reduce the likelihood of you becoming the victim.

What is phishing?

Phishing aims to lure individuals into inadvertently revealing their credentials (e.g. passwords) for both personal and work accounts. To achieve this, attackers might send legitimate-looking password reset emails, urgent-sounding messages about financial problems, account change notifications requests, or links to documents that require you to log in with passwords. The emails are very convincing and could arrive at an individual's personal or work email account, perhaps even appearing to come from someone known to the recipient.

Why is the NCSC concerned?

The NCSC has become aware of phishing attacks to gain access to the online accounts of:

- individuals that were MPs before dissolution of parliament
- other staff who work in political parties

Phishing attacks are likely to continue and may be sent to parliamentary email addresses, prospective parliamentary candidates, and party staff.

How do I know if I've been attacked?

Look through your inbox and see if you have received emails purporting to be from an online service since January 2017. These might be **unexpected** requests to reset your password for online or social media accounts (such as Apple, Google, Microsoft, Facebook or Twitter). Or you might have been asked to approve changes to your account that you've not requested.

What should I do if I think I've been attacked?

- **Immediately report anything suspicious**. If you think you've received a fake email, do not click on any links. Report it immediately to your organisation's IT team, and to your service provider. You should also forward the fake email to samples@analysis.ncsc.gov.uk.
- **If you've already clicked on a suspicious link**, the same rules above apply. Contact your IT team immediately and inform the NCSC incident team (incidents@ncsc.gov.uk).
- **Change the password of the online service** as the attacker may still have access. If you're using the same (or similar) passwords on *other* accounts, change these as well. You can find advice on passwords at www.cyberaware.gov.uk/passwords.
- **Check if any unknown devices have logged onto your accounts**. This is normally visible on the security pages of your account. If you have the option to, you should disconnect devices that you don't recognise.
- **Enable multi-factor authentication** (also known as two-step or two-factor authentication) on your email and social media accounts. Your IT team will be able to help you do this, or you can refer to the support pages below.

Help with multi-factor authentication

For more information about how to enable multi-factor authentication for common online services, please refer to the following:

- **Google (including email)** (https://www.google.com/landing/2step/)
- **Facebook** (https://www.facebook.com/help/148233965247823?helpref=faq_content)
- **Apple (including iCloud)** (https://support.apple.com/en-gb/HT204152)
- **Yahoo** (https://help.yahoo.com/kb/SLN5013.html)
- **Microsoft (including Hotmail)** (https://support.microsoft.com/en-gb/help/12408/microsoft-account-about-two-step-verification)
- **Twitter** (https://support.twitter.com/articles/20170388)

What can I do to prevent being a victim of phishing attacks?

Phishing attacks can be hard to prevent due to the convincing nature of the fake emails, but there are simple steps you can take to significantly reduce the risk of becoming a victim.

- **Enable multi-factor authentication**, as described above.
- **Look out for unexpected emails**.
- **Immediately report anything suspicious**, especially if you've already clicked.

Advice for IT departments

The following recommendations will reduce the likelihood of your organisation becoming a victim of phishing attacks. If your organisation needs further help, we recommend that you contact an NCSC-certified Cyber Incident Response Company.

- Tell users about the threat from phishing attacks. Use the recent En Marche hack as an example that can make your communications more effective.
- Help users to enable multi-factor authentication on important accounts (both personal and work), and emphasise the importance of swift reporting of anything suspicious (especially if they have already clicked).
- Encourage users to ask for help if they believe they may have been a victim of phishing in the past (and have not raised it to date).
- Recognise that attacks to get information stored in users' personal accounts may be just as damaging as information held inside your organisation's IT. Encourage use of organisational IT to discuss work matters wherever possible.
- Ensure that the services you use (such as email, document stores, collaboration tools etc.) all allow for multi-factor authentication. If this is not possible, restrict access to your services to known devices.
- Carefully consider your remote access strategy, and how you will identify unusual or unexpected access or behaviour (such as downloading an inbox).
- Ensure your security operations team have access to all the data sources they require to quickly spot and respond to potential phishes, and are empowered to take urgent action to protect users and information in a timely fashion.
- If you've not already done so, have key phishing mitigations in place (such as disallowing internet browsing from admin accounts, making easy reporting mechanisms for users, and rehearsing incident response).
- If a user believes their personal account has been compromised, you can assist by asking the user to forward the suspicious email, making a password change, enabling multi-factor authentication, viewing (and validating) device logins, terminating current sessions, and understanding what information may have been lost. Providers may support a subset of these steps, please check directly with the provider.