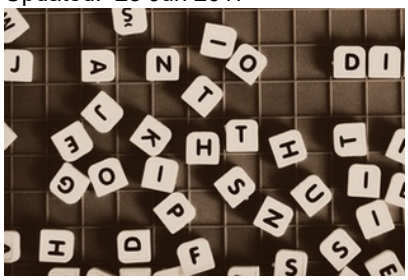
National Cyber Security Centre
a part of GCHQ

Guidance (/)

Password guidance summary: how to protect against password-guessing attacks

Created: 28 Jun 2017
Updated: 28 Jun 2017



How organisations and individuals can protect themselves from password-guessing attacks.

Recently, the NCSC have seen an increase in a number of incidents, and also more press reporting around historic password compromises (https://www.theguardian.com/technology/2017/jun/23/russian-hackers-stole-passwords-of-british-mps-and-public-servants). In light of this, we're taking this opportunity to summarise the salient points from our password guidance(/guidance/password-collection) that relate specifically to how you can protect against password-guessing attacks.

- If attackers are able to access your systems remotely by guessing users' passwords, then those systems are not effectively protected; don't blame the users in this situation.
- Forcing regular password resets is counter-productive(/blog-post/your-password-expiry-policy-may-have-reached-its-expiry-date), but that doesn't mean they're never needed(/blog-post/linkedin-2012-hack-what-you-need-know). Make sure your users know how to reset their passwords when this is necessary, and help them pick hard-to-guess passwords(/blog-post/three-random-words-or-thinkrandom-0).
- Prevent password-guessing attacks by setting up multi-factor authentication for your users on all the enterprise services used across your organisation. Encourage your users to do the same for their personal services. All major providers have advice on how to do this (see below), or your IT staff can help.
    - **Google** (including gmail) https://www.google.com/landing/2step/ (https://www.google.com/landing/2step/)
    - **Facebook** https://www.facebook.com/help/148233965247823?helpref=faq_content (https://www.facebook.com/help/148233965247823?helpref=faq_content)
    - **LinkedIn** https://www.linkedin.com/help/linkedin/answer/544/turning-two-step-verification-on-and-off?lang=en (https://www.linkedin.com/help/linkedin/answer/544/turning-two-step-verification-on-and-off?lang=en)
    - **Apple** (including iCloud) https://support.apple.com/en-gb/HT204152 (https://support.apple.com/en-gb/HT204152)
    - **Yahoo** https://help.yahoo.com/kb/SLN5013.html (https://help.yahoo.com/kb/SLN5013.html)
    - **Microsoft** (including Hotmail) https://support.microsoft.com/en-gb/help/12408/microsoft-account-about-two-step-verification (https://support.microsoft.com/en-gb/help/12408/microsoft-account-about-two-step-verification)
    - **Twitter** https://support.twitter.com/articles/20170388 (https://support.twitter.com/articles/20170388)
    - **Dropbox** https://www.dropbox.com/help/security/enable-two-step-verification (https://www.dropbox.com/help/security/enable-two-step-verification)
    - **Instagram** https://help.instagram.com/566810106808145 (https://help.instagram.com/566810106808145)
    - **Amazon** https://www.amazon.com/gp/help/customer/display.html?nodeId=201962420 (https://www.amazon.com/gp/help/customer/display.html?nodeId=201962420)
    - **Box** https://community.box.com/t5/How-to-Guides-for-Account/Can-I-Enable-2-Step-Verification-For-My-Box-Account/ta-p/29 (https://community.box.com/t5/How-to-Guides-for-Account/Can-I-Enable-2-Step-Verification-For-My-Box-Account/ta-p/29)

Remind your users to:

- **Always use unique passwords for your work accounts**. Always change them immediately, and report it, if you think they may have been compromised or you notice anything else suspicious.
- **Store your passwords** rather than trying to remember them all. This enables you to use longer, stronger, unique passwords and change them whenever you want, without making life too hard for yourself. There are two ways you can do this:
    - **Use a password manager**. These can easily create and maintain long, complex, unique passwords for every service you use. Read our blogpost on password managers(/blog-post/what-does-ncsc-think-password-managers) to help you pick a reputable product, and use it in accordance with any instructions provided by your IT staff.
    - Alternatively, **write your passwords down** on a piece of paper that you guard very carefully (and keep separate from the devices they relate to). Disguise them if you can, and don't write your usernames alongside the passwords.

- **When creating passwords, make sure they can't be easily guessed by people who know you**, or derived from information gleaned from your social media profiles. Avoid the use of single dictionary words, or variations of these - use three random words(/blog-post/three-random-words-or-thinkrandom-0) instead. Don’t bother replacing the letter 'O' with a zero (or replacing the letter 'I' with the number one) or any other techniques as hackers can exploit these rules.

Where to get extra help

For more information, please see the NCSC’s guidance on passwords for system administrators(/guidance/password-guidance-simplifying-your-approach).

Topics

Identity and passwords(/topics/identity-and-passwords)
Cyber threats(/topics/cyber-threats)

Was this guidance helpful?

We need your feedback to improve this content.

Yes No