[FRONTCOVER]

Cyber aware

National Cyber Security Centre alternative formats edition

Lead Scotland
Linking education and disability
Lead.org.uk
enquiries@lead.org.uk

Cyber aware

National Cyber Security Centre alternative formats edition.

This document has been produced by Lead Scotland in conjunction with partners and with funding from the Scottish Government Cyber Resilience Unit in conjunction with Lead Scotland.

This guide is based on the content available at National Cyber Security Centre.

Using the alternative formats version

Note: Full web address links are written in full in the appendix and organised by subheadings of this document. This may be beneficial for readers accessing the information when published in printed, braille or audio format.

Detailed content and additional information are provided in the appendix to help with flow and understanding.

Styles have been used to indicate structure and to allow adaption to individual reading preferences.

Version:0.2

Date released:19/03/2021

6 ways to improve your online security

Due to coronavirus, people are spending more time online this year.

This means more opportunities for hackers to carry out cyber-attacks. They often do this by targeting people and businesses using:

- Email and website scams.
- Malware - software that can damage your device or let a hacker in.

If hackers get into your device or accounts, they could access your money, your personal information, or information about your business.

You can improve your cyber security by taking six actions:

Action 1 - Use a strong and separate password for your email.

Action 2 - Create strong passwords using 3 random words.

Action 3 - Save your passwords in your browser.

Action 4 - Turn on two-factor authentication (2FA).

Action 5 - Update your devices.

Action 6 - Back up your data.

ACTION 1 - Use a strong and separate password for your email

If a hacker gets into your email, they could:

- Reset your other account passwords.
- Access information you have saved about yourself or your business.

Your email password should be strong and different to all your other passwords. This will make it harder to crack or guess.

Using three random words is a good way to create a strong, unique password that you will remember.

You should also protect your other important accounts, such as banking or social media.

VIDEO: Why email is so important

A transcript of the ‘Why email is so important’ video is available in the appendix.

Access the video covering "Why email is so important" online.

Did you know?

If a hacker gets into your email, they could reset the passwords for your other accounts using the ‘forgot password’ feature.

How to change your email password

How to change your password in:

- Gmail.
- Yahoo!.
- Outlook.
- BT.
- AOL Mail.

If your email is not listed here, you should search online for advice from your provider on how to change your email password.

Advice on passwords for sole traders and small businesses

If you are a business owner, your accounts may include sensitive information about your customers, your business, or your finances.

If your accounts are not secure, your business could be more at risk of a cyber incident. This may put your business at legal or financial risk, and at risk of breaking the General Data Protection Regulation (GDPR).

If your business has staff, you should make sure they do not store their passwords next to their devices, and that devices are locked or turned off when not in use.

For more information, see our Small Business Guide.

ACTION 2 Create strong passwords using three random words

When you use different passwords for your important accounts, it can be hard to remember them all.

A good way to create strong, memorable passwords is by using three random words.

Do not use words that can be guessed (like your pet's name). You can include numbers and symbols if you need to. For example: "RedPantsTree4!"

Saving your passwords in your browser will help you manage them.

Test your knowledge for creating a strong password

Question: Which one of these passwords does not appear in the top 100,000 most compromised passwords?

- arsenal22
- 1v&upjw3nt
- p@55w0rd
- RedPantsTree
- Victoria!
- 2011977

Answer Creating a strong password

The answer is RedPantsTree.

Hackers share online lists containing millions of compromised passwords.

3 random words is an easier way to create new passwords that are more likely to be unique to you and less likely to be guessed.

ACTION 3 Save your passwords in your browser

Saving your password in your browser means letting your web browser (such as Chrome, Safari or Edge) remember your password for you.

This can help:

- Make sure you do not lose or forget your passwords.
- Protect you against some cyber-crime, such as fake websites.

It is safer than using weak passwords or using the same password in more than one place.

Make sure you protect your saved passwords in case your device is lost or stolen.

How to protect your saved passwords

Someone who gets access to your device may be able to use your saved passwords to access your accounts.

This kind of cyber-crime is much less common than remote attacks over the internet, where passwords are cracked using software.

To make sure you are protected, you should:

- Turn off or lock your device when you are not using it.
- Use a strong password to protect your device.
- Turn on two-factor authentication for all your devices and accounts.
- Turn on biometrics (Face ID or Fingerprint recognition) if your device supports this.

You should also back up your data regularly. This will help you recover your important information if your device is lost or stolen.

How to save your passwords in your browser

Find out how to save your passwords in:

- Google Chrome.
- Microsoft Edge.
- Firefox.
- Safari.

Did you know?

You can access your saved passwords from any device where you are signed into the same browser.

Add extra protection

Once you have set up strong, separate passwords (Actions 1 to 3) for all your devices and services, there are other things you can do to reduce your risk of being hacked (Actions 4 to 6).

ACTION 4 Turn on two-factor authentication (2FA)

Two-factor authentication (2FA) helps to stop hackers from getting into your accounts, even if they have your password.

Some online banking uses 2FA automatically. It does this by asking for more information to prove your identity, such as a code that gets sent to your phone.

How to turn on two-factor authentication (2FA)

You will need to manually turn on 2FA for most of your accounts. Not all accounts will offer 2FA. Online banking uses 2FA automatically.

2FA is also known as two-step verification or multi-factor authentication.

VIDEO: How 2FA works

A transcript of the “How 2FA works” video is available in the Appendix.

Access to the video on How 2FA works is available on YouTube.

Turn on 2FA for email

- Gmail.
- Yahoo.
- Outlook.
- AOL.

Turn on 2FA for social media

- Instagram.
- Facebook .
- Twitter.
- LinkedIn.

ACTION 5: Update your devices

Out-of-date software, apps, and operating systems have weaknesses. This makes them easier to hack.

Companies fix the weaknesses by releasing updates. When you update your devices and software, this helps to keep hackers out.

Turn on automatic updates for your devices and software that offer it. This will mean you do not have to remember each time.

Some devices and software need to be updated manually. You may get reminders on your phone or computer. Do not ignore these reminders. Updating will help to keep you safe online.

How to turn on automatic updates

Find out how to turn on automatic updates for:

- Apple - Mac
- Apple - iPhone and iPad
- Microsoft Windows 10. – Search Windows 10 for update
- Windows 7 is no longer supported. You should upgrade to Windows 10
- Android smartphones and tablets
- Android apps

Test your knowledge: How do companies fix weaknesses in their software?

Question: How do companies fix weaknesses in their software?

- Bandage
- Patch
- Repair

Answer: When a company finds a weakness in their software, they release a 'patch' to fix it. This helps to keep your information secure.

ACTION 6 - Back up your data

Backing up means creating a copy of your information and saving it to another device or to cloud storage (online).

Backing up regularly means you will always have a recent version of your information saved. This will help you recover quicker if your data is lost or stolen.

You can also turn on automatic backup. This will regularly save your information into cloud storage, without you having to remember.

If you back up your information to a USB stick or an external hard drive, disconnect it from your computer when a backup isn't being done.

Did you know?

You should always back up your data before updating your device.

This is because updates can sometimes remove or change files.

How to turn on automatic backup

How to turn on automatic backup for:

- Apple – Mac.
- Apple - iPhone and iPad.
- Android.
- Microsoft Windows 10 and Windows 8 OneDrive.

Advice on backups for sole traders and small businesses

Backing up your data will mean your business can continue to operate if a cyber incident does happen.

Start by identifying the data that is most important to your business. This could be financial, contract, customer, or supplier information. Make sure it is backed up regularly.

You should also know how to restore a backup in the event of data loss.

For more information, see our Small Business Guide.

More tips on how to stay safe online

Phishing: How to report to NCSC.

Discover how to report a potential phishing message to the NCSC using the Suspicious Email Reporting Service (SERS).

Shopping online securely

Our guidance will help you to avoid scam websites and purchase items safely.

[END OF MAIN DOCUMENT – APPENDIX FOLLOWS]

Appendix

Video: Why email is so important - Transcript

Why email is so important video available at https://youtu.be/lYq5-p6Ovd0.

Email is one of your most important accounts. But why do hackers care about your emails?

Imagine a hacker gets into your email

They can now access information you have saved about yourself

or contact people pretending to be you

But worst of all, they can lock you out of any of your online accounts

They can do this by going to any of your accounts and using the ‘forgot password’ feature

This sends an email with a link to reset your password

Which the hacker can use to lock you out of your account

Once they’ve reset one password, they can continue to reset passwords for your other accounts too

So, how can you protect your email and help to keep hackers out of all your online accounts?

Use a separate and strong password for your email

"Do not use words that can be guessed like your pet’s name or favourite football team. Using 3 random words will help you create passwords that are long and difficult to guess.

Make sure the password for your email is different to all your other passwords that you use"

This means that if someone cracks your password for another account, they won’t be able to use this to get into your email

Remember, your email is one of your most important accounts. Make sure it’s secure

Video: How 2FA works.

How 2FA works video available at https://youtu.be/zD-CNuMxn5Q.

When you log into a website or app with 2fa

It will ask you to prove you are really you

It may send you a code

Then, if you're able to provide this

You can log in and use the service

Links in Full

Introduction Section links

National Cyber Security Centre - https://www.ncsc.gov.uk/cyberaware/home#action-1

ACTION 1 Links - Use a strong and separate password for your email.

Why email is so important Video is available online - https://youtu.be/lYq5-p6Ovd0

How to change your password in

- Gmail -https://support.google.com/accounts/answer/41078.
- Yahoo! - https://help.yahoo.com/kb/account/reset-yahoo-password-sln27051.html.
- Outlook - https://support.microsoft.com/en-gb/office/change-your-password-in-outlook-com-2138d690-811c-4545-b2f3-e4dbe80c9735?ui=en-us&rs=en-gb&ad=gb.
- BT - https://www.bt.com/help/email/manage-email-account/i-need-to-change-or-reset-my-bt-email-password.
- AOL Mail - https://help.aol.co.uk/articles/account-management-managing-your-aol-password.

Small Business Guide - https://www.ncsc.gov.uk/collection/small-business-guide.

ACTION 2 links- Create strong passwords using 3 random words-

No Links used

ACTION 3 links -Save your passwords in your browser-

Find out how to save your passwords in:

- Google Chrome - https://support.google.com/chrome/answer/95606?co=GENIE.Platform%3DDesktop&hl=en&oco=1.

- Microsoft Edge - https://support.microsoft.com/en-us/microsoft-edge/save-or-forget-passwords-in-microsoft-edge-b4beecb0-f2a8-1ca0-f26f-9ec247a3f336.
- Firefox - https://support.mozilla.org/en-US/kb/password-manager-remember-delete-edit-logins#w_make-firefox-remember-usernames-and-passwordsSafari - https://support.apple.com/en-gb/guide/mac-help/mchlf375f392/mac.

ACTION 4 links Turn on two-factor authentication (2FA)

How 2FA works is available at YouTube - https://youtu.be/zD-CNuMxn5Q.

Turn on 2FA for email

- Gmail - https://myaccount.google.com/signinoptions/two-step-verification/enroll-welcome?pli=1.
- Yahoo - https://help.yahoo.com/kb/add-two-step-verification-extra-security-sln5013.html.
- Outlook - https://support.microsoft.com/en-us/account-billing/how-to-use-two-step-verification-with-your-microsoft-account-c7910146-672f-01e9-50a0-93b4585e7eb4.
- AOL - https://help.aol.com/articles/2-step-verification-stronger-than-your-password-alone?guccounter.

1Turn on 2FA for social media

- Instagram - https://help.instagram.com/1124604297705184.
- Facebook - https://www.facebook.com/help/148233965247823.
- Twitter - https://help.twitter.com/en/managing-your-account/two-factor-authentication.
- LinkedIn - https://www.linkedin.com/help/linkedin/answer/544/turn-two-step-verification-on-and-off?lang=en.

ACTION 5: Update your devices

Find out how to turn on automatic updates for:

- Apple - Mac https://support.apple.com/en-gb/HT202180.
- Apple - iPhone and iPad https://support.apple.com/en-gb/HT204204.
- Microsoft Windows 10. - Search Windows 10 for update.

- Windows 7 is no longer supported. You should upgrade to Windows 10 https://computing.which.co.uk/hc/en-gb/articles/360009159719-How-to-upgrade-from-Windows-7-to-Windows-10-for-free.
- Android smartphones and tablets - https://support.google.com/android/answer/7680439?hl=en-GB
- Android apps - https://support.google.com/googleplay/answer/113412?hl=en-GB.

ACTION 6 - Back up your data

- Apple - Mac https://support.apple.com/en-gb/mac-backup.
- Apple - iPhone and iPad https://support.apple.com/en-gb/HT203977.
- Android - https://support.google.com/android/answer/2819582?hl=en-GB.

Microsoft Windows 10 and Windows 8 OneDrive - https://support.microsoft.com/en-us/office/turn-on-onedrive-backup-4e44ceab-bcdf-4d17-9ae0-6f00f6080adb.

Advice on backups for sole traders and small businesses

Small Business Guide - https://www.ncsc.gov.uk/collection/small-business-guide.

Additional Information

Suspicious Email Reporting Service (SERS).
https://www.ncsc.gov.uk/information/report-suspicious-emails.

Our guidance will help you to avoid scam websites and purchase items safely. - https://www.ncsc.gov.uk/guidance/shopping-online-securely.

Lead Scotland
Linking education and Disability

Lead Scotland
525 Ferry Road
Edinburgh
EH5 2FF
T 0131 228 9441

enquiries@lead.org.uk
www.lead.org.uk

[END OF DOCUMENT]