Bexley Digital Champions Network

Staying Safe Online

Today’s Training

1. Downloading Apps
2. QR Codes
3. Ask Silver
4. Online safety tips
5. Password Management
6. More digital support in Bexley

Downloading Apps

- Applications (Apps) are an easy way to access most of what we need online.
- They provide quick access to your favourite websites.
- You can have as many as you like!
- Most apps are free.
- Apps should never need your bank details – only an email address and password to log in. Use different passwords for things!

App store logo

Google play logo

You may be asked to provide credit card details when using the app store – this is only needed if you are buying paid apps – otherwise you can close the pop-up.

Quick Response (QR) Codes

- codes are ‘links’ that can help you to access specific information on the Internet more quickly.
- QR codes are often used to provide access to online services.
- QR codes are accessed by ‘holding’ your device’s camera over the image and then tapping on the link, when shown.
- QR codes can be used on Apple and Android devices.
- Some Android devices may require you to download an app (QR Reader).

Check that the link (URL) makes sense before you click on it!

Ask Silver

- Receive scam alerts
- Silver sends out regular alerts about the latest scams
- Submit scams for analysis
- You can take a photo or screenshot of any email, website, or leaflet you're worried about and send it to Silver
- Report scams in a second
- You can ask Silver to report the scam to relevant agencies on your behalf

You will need to know how to use WhatsApp and how to take a screenshot to use this

Taking a screenshot

Android:

Power and Volume Down:

Simultaneously press and hold the power button and the volume down button. The screen will flash, indicating a screenshot has been taken.

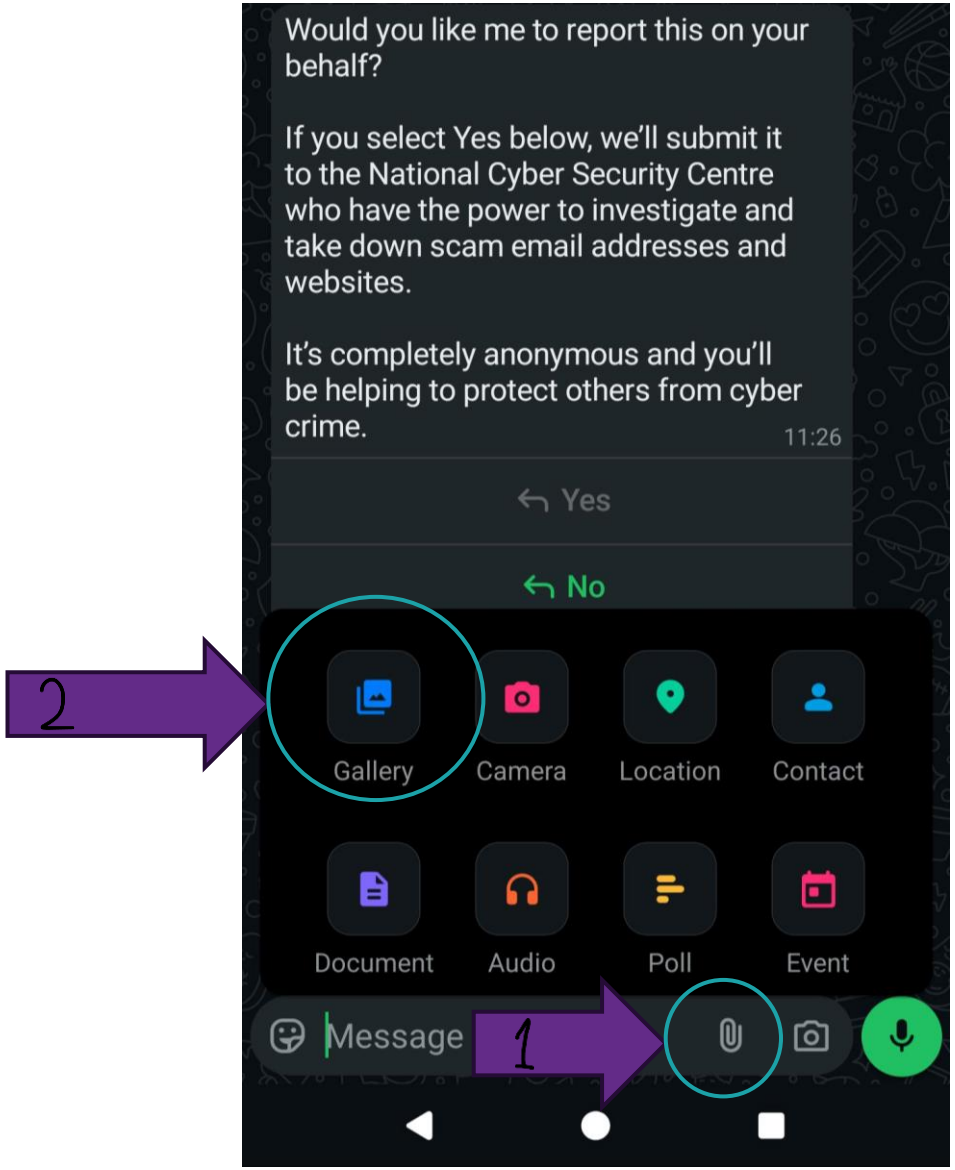
iPhone:

Side Button and Volume Up:

Simultaneously press and release the side button and the volume up button.

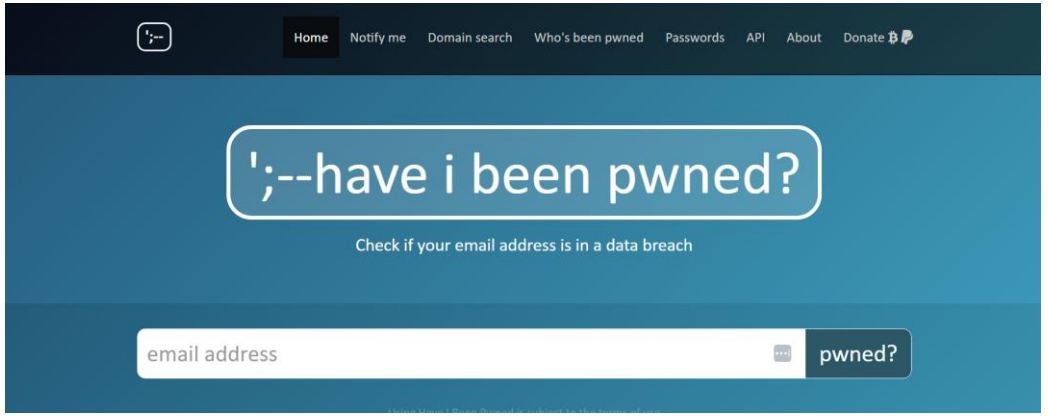
Sending an image in WhatsApp

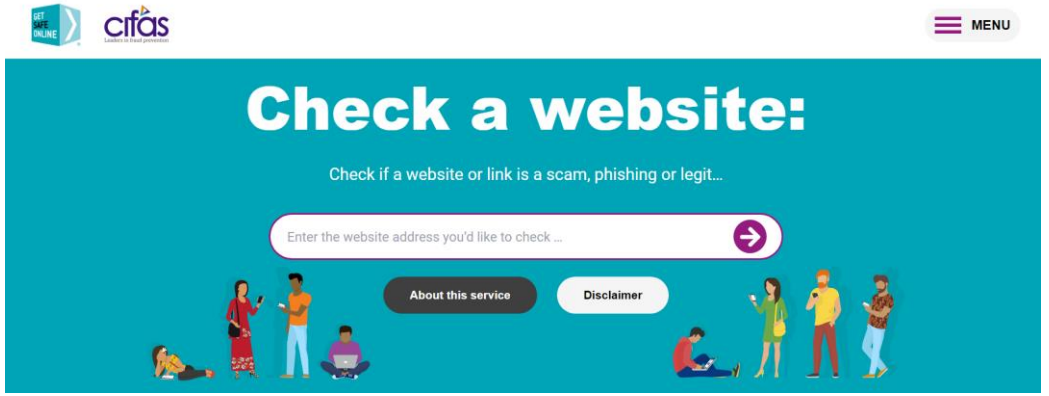
1. Open the chat on WhatsApp
2. Click the attachment icon – the paperclip
3. Click “Gallery” on the pop-up options
4. Select the relevant photo.



Some tips to help you stay safer online

- Make sure Anti-virus software is up to date
- Use passwords that are not easily guessed
- Beware of selecting any links within emails/messages/social media that require your card or bank details.
- getsafeonline.org and haveibeenpwned.com
- Stop and Think! – If someone is rushing you, then it's probably fraudulent.





- Don’t click on links in emails from unfamiliar senders. Be wary of any strange or unexpected messages, even if it's from someone you know.
- Don’t open any attachments unless you know the sender and were expecting them to send it.
- Ignore unsolicited phone calls and “robocalls.”
- Don’t respond to or click on pop-up windows on your phone or computer.
- Don’t conduct any transaction involving personal information while using a public (or unsecured) network

Fake Websites

Scammers set up fake websites as a way to get your personal information.

This could be a fake banking website where they ask you to update your details or account information, for example.

There are also websites set up to get you to pay for free services.

These are usually government services, such as renewing your passport.

These websites aren't illegal but are set up to make you pay for free services.

Top tip

Don't fill out any personal details or make any transactions on a website until you're sure it's safe. If online banking, always search for the website yourself.

You should look out for:

Although these websites are designed to look very similar, look out for any details of the website that don't look quite right.

Email scams

Scammers send emails to try and get you to give them your personal details.

They might either try and direct you to a fake website, claim something's wrong with an account or device you own or claim you've won a prize.

Sometimes there might be a file attached to the email.

The scammer wants you to open or download this as it could harm your device by releasing or downloading a virus (malware).

Top tip

Don't open any attachment or click on any links that you're suspicious of.

You should look out for:

- Errors in the spelling or grammar, or wording that just doesn't seem quite right.
- Requests for personal information, such as usernames, password or bank details.
- Anything that's time-sensitive and wants you to act fast.

Other types of scams

Health scams

- Scammers make false or misleading claim about certain products, such as miracle cures.
- These medicines can be expensive, poor quality and in some cases even harmful.

Relationship Scams

- Some people will use social media or dating websites to contact you.
- They try to gain your trust and then might start asking for money, often by telling an emotional story.
- These can be hard to spot, especially for those directly involved, so it’s always good to talk to someone else about the situation if you’re suspicious.
- Never send personal or financial details.
- Remember that people can use AI now to create fake videos and photos to convince you that they’re real.

Password Management

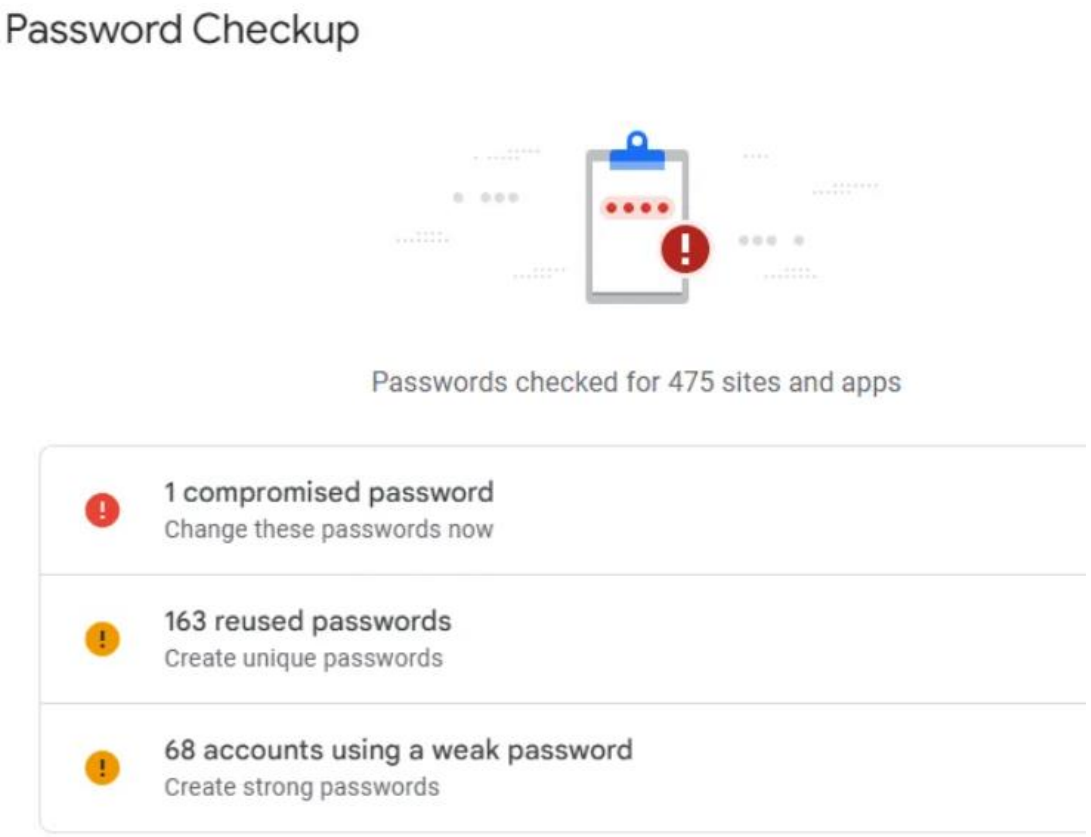
- It’s really important to not use the same password for multiple sites. Password managers are built into most phones and browsers now; these are helpful because they:

- **Stores all your passwords safely** – You only need to remember one master password instead of many different ones.

- **Fills in passwords for you** – It can automatically enter your saved passwords on websites, saving time and effort.

- **Creates strong, unique passwords** – Helps you make secure passwords that are hard for hackers to guess.

- **Keeps your information safe** – Uses strong encryption to protect your data from being accessed by others.



Google has their own inbuilt password manager which also performs password checks, so you see **compromised passwords** involved in known data breaches, **weak passwords** that should be upgraded, and the sites where you've **used the same password** more than once.

Digital Support in Bexley!

There is a fantastic team of digital volunteers throughout Bexley who can support with the NHS app and loads more!

Find more info on our website:

https://www.bvsc.co.uk/bexley-digital-champion-network-0