BEXLEY DOMESTIC ABUSE SERVICES

CYBER SAFETY ADVICE

Sections include:
- Secure your video calling
-Secure your email account
-Privacy on the web

SECURE YOUR VIDEO CALLING: WhatsApp / Messenger / Houseparty

WhatsApp *(for Google Android & Apple iOS)*

WhatsApp is possibly the most popular messaging app around, in order to maintain some privacy, you may want to change your last seen privacy settings in WhatsApp. Here's how you do it:

Google Android

1. Launch **WhatsApp** from your Home screen or the app drawer.
2. Tap on the **More options** button (it looks like three dots aligned vertically and is in the top right-hand corner of your screen).
3. Tap on **Settings**
4. Tap on **Account**
5. Tap on **Privacy**
6. Tap on **Last seen.**
7. Choose whatever option you want:
   Everyone: All WhatsApp users get Last seen updates about you.
   My contacts: Only people on your contacts list get Last seen updates.
   Nobody: Other WhatsApp users will no longer get any Last seen updates about you.

Apple iOS

1. Launch **WhatsApp** from your Home screen.
2. Tap on the **Settings** tab (it's the little gear icon in the bottom right corner of your screen).
3. Tap on the **Account** button (it's the blue box with the white key in the middle).
4. Tap on the **Privacy** button.
5. Tap on the **Status** button. This will show you a menu with three options.
   Everyone (This means anyone on WhatsApp can see it, this is the default setting)
   My Contacts (This means only people you have in your contacts)
   Nobody (This means no one can see this info)
6. Tap on the option you desire.

Messenger

The appeal of Messenger is that it is attached to Facebook and so can be linked to a user's friends even if they aren't in their phone contacts. It can be used for voice and video calling but, unlike WhatsApp, it currently doesn't use end-to-end encryption.

To access the security setting in Messenger for both Google Android and Apple iOS, follow the steps below:

1. Login to **Facebook Messenger.**
2. Check the **top right corner** of Facebook Messenger.
3. Tap your **profile picture**.
4. Scroll down until you get to **Account Settings.**
5. Tap **Account Settings.**
6. You now have access to Security within Account Settings.

Houseparty *(for Google Android & Apple iOS)*

Houseparty has millions of downloads during the coronavirus pandemic and it has become a very popular video socialising app. However, from a privacy perspective, there's one obvious issue that you may want to take note of before organising games and parties: they are open to any of your friends and friends of friends unless you lock the "room" where you're playing. Here's how you can secure that feature:

Google Android
To lock all rooms that you enter by default:

1. Tap on **Account.**
2. Tap on **Settings.**
3. Tap the **Private Mode** toggle to on.

Apple iOS

1. Once in a chat, tap the three vertical dots at the bottom left of the screen.
2. **Tap the padlock** to Lock the Room.

SECURE YOUR EMAIL ACCOUNT: Passwords /Two Factor Authentication

Passwords

There are many different email vendors on the web, but they all offer many features to secure your account. In a situation where email accounts have previously been shared, it is a good idea to create a new account to ensure that an ex-partner no longer has access to your emails. An email account is where we hold all of our important business: shopping confirmations, banking messages and, most importantly, password reset requests. With unauthorised access to an email account, a password can be reset for almost all other accounts.

Two ways in which you can greatly reduce the risk of your email account being compromised are having a strong password and using two factor authentications. Here's how to do these:

To create a strong password:
This needs to be memorable but also strong. To do this, come up with your own formula to replace some of the letters with numbers.

Here is an example of letters that are replaced by numbers based on their similarity:

A = 4
E = 3
I = 1
O = 0
S = 5
Z = 2

Think of a place and date that has meaning to you:

Amsterdam 26th March 1996

In order to create that memory into a secure password, just take it through two simple stages:

Remove all the spaces and convert the date: **Amsterdam260396**
Apply the above formula: **Am5t3rd4m260396**

If you wish to add an extra layer of security to your password, or if it is required of the site that you are setting an account up for, you can add in a symbol too:

$Am5t3rd4m260396

App stores also offer password generator apps, should you wish to create random, strong passwords. However, you will need a way of remembering these once generated!

Two Factor Authentication (2FA)

What is Two Factor Authentication?

This is an extra layer of security which guarantees a more secure account for you online.

Popular authenticators include:

- Google Authenticator
- LastPass Authenticator
- Microsoft Authenticator
- Authy
- Yubico Authenticator

Many apps and websites have 2FA built in as an option, but you have to find it in the settings.

Except for online banking, it is rarely switched on as a default, but it is extremely important to use this feature wherever it is offered.

Some banks use card readers or PIN pads to allow account holders to log in to their accounts, others text or phone a code to their registered device. With other services, such as email accounts or subscriptions, you may be given the option to either receive a text code or use an authentication app.

These apps are available to download for free from the app stores, and the most popular are **Google Authenticator** and **Microsoft Authenticator**. However, there are many others and you may be asked to use a particular one.

What to do before setting up setting up a 2FA

- Google Authenticator has been downloaded from the Google Play Store (Google Android) or the App Store (Apple iOS).

- A barcode or QR scanner is installed on your phone. If one isn't, Google Authenticator will ask you
- to do so.

- You have a Google account set up (other authenticator apps do not require this).

- You have visited the site or app that is requesting the 2FA setup.

EXAMPLE – How to setup a 2FA on Google Authenticator for a Facebook Account

1. On your phone, open the **Facebook** app

2. Tap the 3 horizontal bars at the **bottom right** of the screen
3. Scroll down and tap **Settings**

4. Scroll down and tap **Security** and login

5. Scroll down to Two-factor authentication and tap **Use two-factor authentication**

6. Scroll down to **Select a security method** and tap **Authentication app**

7. You'll see the following pages with a QR code at the top and some instructions below

8. To set up the 2FA on a different device, **scan the QR code** with a QR scanner

9. To set up the 2FA on the same device that the Facebook account is logged in to, tap. Set up on same device. You should be prompted to open the Google Authenticator app.

10. If you are offered a different installed authentication app, you can use that one and follow the instructions or enter the code into Google Authenticator manually:

    • Tap and hold the **long code** under or **enter this code** into your authentication app

    • Once the code has been copied (a popup will tell you), open the Google Authenticator app

    • In the Google Authenticator app, **tap the plus symbol** at the top right of the screen and select **Manual entry**

    • Enter the details for the Account (e.g. Facebook username)

    • Paste the details of the code copied in the first stage above into the Key

    • Keep the Time-based toggle switched to **On** (it is by default)

    • Return to the Facebook app where you will be asked to enter the current 6-digit code for Facebook showing in the Google Authenticator app

    • You will then be asked to re-enter your Facebook login password to complete the 2FA setup

You will now be able to use the Google Authenticator app whenever Facebook senses a login.

PRIVACY ON THE WEB: Microsoft Edge / Google Chrome / Firefox / Safari

Web Browsers

There are a number of different web browsers that can be used to access the information on the worldwide web, but the most commonly used are Microsoft's Edge (formerly Internet Explorer), Google Chrome, Mozilla Firefox and Apple's Safari.

Your web browsing history holds valuable information, not only for the commercial businesses that thrive on targeted sales but also for anyone who has unauthorised access to an account linked to your web browser.

For example, if you are logged in to a Google account and search the web using Google search, then your history will be stored at Google by default until you make changes (it can be disabled on your account). If someone has access to your Google account (or, indeed, your device), they will also be able to see exactly what you have been looking at on the web, and this can be useful information for them in certain circumstances.

The easiest way to avoid this is to search the web in a private browsing mode. This will allow you to browse the web without your browser saving any browsing history, cookies and passwords. However, your browsing will still be visible to your Internet Service Provider and your employer, should you be using a work device.

Here's how you can browse privately:

Microsoft Edge

WINDOWS

1. Open **Microsoft Edge**
2. Click on the 3 horizontal dots in the top right of the window
3. Click on **New InPrivate window**
4. Start browsing privately

ANDROID / iOS

1. Open **Microsoft Edge**
2. Tap on the 3 horizontal dots in the bottom right of the screen
3. Tap on **New InPrivate** tab
4. Start browsing privately

Google Chrome

WINDOWS / MAC OS

1. Open **Google Chrome**
2. Click on the 3 vertical dots in the top right of the window
3. Click on **New incognito window**
4. Start browsing privately

Tip - Keyboard shortcuts to open an incognito window: Ctrl-Shift-N (Windows) or Command/cmd-Shift-N (Mac)

ANDROID / iOS

1. Open **Google Chrome**
2. Tap on the **tabs** icon in the top right of the screen
3. Tap on the 3 vertical dots in the top right of the screen
4. Tap on **New Incognito Tab**
5. Start browsing privately

Mozilla Firefox

WINDOWS / MAC OS

1. Open **Mozilla Firefox**
2. Click on the 3 horizontal lines in the top right of the window
3. Click on **New Private Window**
4. Start browsing privately

Tip - Keyboard shortcuts to open a new private window: Ctrl-Shift-P (Windows) or Command/cmd-Shift-P (Mac)

ANDROID / iOS

1. Open **Mozilla Firefox**
2. Tap on the **tabs** icon in the top right of the screen
3. Tap on the **mask icon** in the bottom right of the screen
4. Tap on **the plus sign (+)** in the bottom left of the screen to open a new tab
5. Start browsing privately

Safari

MAC OS

1. Open **Safari** from the dock
2. Click on **File** in the top left of the Safari menu bar
3. Select **New Private Window** from the list
4. Start browsing privately

Tip - Keyboard shortcut to open a new private window: Command/cmd-Shift-N

iOS MOBILE

1. Open the **Safari** app
2. Tap on **the tabs** icon in the bottom right of the screen
3. Tap on **Private** in the bottom left of the screen
4. Tap on the **plus sign (+)** in the bottom centre of the screen to open a new tab
5. Start browsing privately

An alternative to making these adjustments is to use a privacy extension to your web browser, such as DuckDuckGo. This will ensure that you browse privately all of the time.