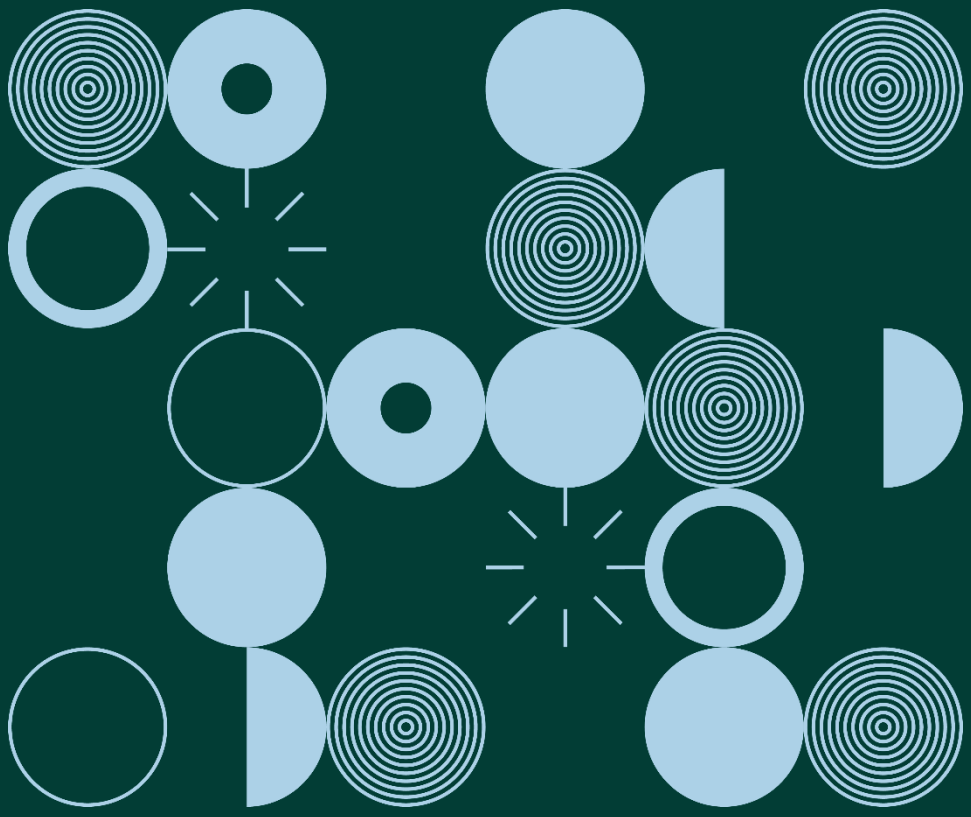
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Guidance Note:

What should you be aware of online? Some common online risks

October 2019



Contents

Introduction

Every day, each one of us as a matter of convenience and utility engages with a variety of websites, apps and social media platforms using our desktop PCs, tablets and smartphones. In doing this, our personal data is being collected and processed in a whole range of ways which we may be unaware of and which may pose some risks to us.

The aim of this note is to help you to be aware of these risks, identify when they can arise, and suggest steps that can be taken to deal with them and protect yourself online. Of course, the more you know, the better equipped you are to keep yourself and your personal data safe and to exercise choice and control in deciding how you engage online with social media and other online services.

Important issues to consider include the amount of tracking or profiling you are willing to accept in order to access apps and services, or the optional features they may offer you. The organisations that create and offer these apps and services to you are known under the General Data Protection Regulation (GDPR) as 'controllers' because they are the organisations that design and determine the ways and means that your personal data is collected and used.

This note focuses on awareness, security, and tracking. The risks mentioned in this note represent those risks that can involve an 'information imbalance' between you and the organisations that provide the sites, apps, and services you use and that have the potential to affect your data protection rights[1].

The descriptions below are not intended as a commentary on organisations' levels of data protection compliance or the effectiveness of the controls they make available, or even on what might be 'best practice'. Instead, this note aims to raise awareness about some of the risks that data subjects might encounter online from time-to-time.

[1] GDPR gives you certain rights regarding your personal data and under certain conditions. These include the right to access or move ("portability") your personal data held by an organisation, a right object to certain processing, a right to erasure, a right to restrict certain processing.

Awareness

Transparency/Purpose Limitation

What to be aware of

When providing information to online services, you may think that the personal data you provide will not be used for anything beyond the process or transaction you are participating in at that particular moment in time.

However, this is not always the case. Personal data provided to online services is often used for other purposes. These should be set out in the organisations' online privacy or data policy. Organisations often describe the immediate purpose or benefit to you at the time you make use of certain features, but also describe other purposes and other processing of your data in their policy documents. For example, you may see 'pop-up' notices or 'help balloons' describing the feature you are using that involves processing your personal data, and it may include a link to 'learn more' or to a section of the organisation's Privacy Policy that describes potential other related uses of your data.

Often, the personal data you hand over is used to enrich a profile that is created about you, your activities, and your interests. This is then used to tailor and target content that is displayed to you on the website or app, or shared among third party advertising platforms in order to decide what advertisements you are most likely to interact with. These ads may appear on the site or app you are using, or later when you visit a different site or app.

Organisations are required by the GDPR to be transparent with you about how your data will be used in a 'clear and plain' manner and must provide you information about how you can exercise your GDPR rights.

What is the risk to you online?

Some organisations may not be fully transparent about the personal data they process, how and why they process that personal data, or how their users can exercise their data protection rights.

An example of this could be that a website's privacy policy may say something like "We use your personal data to improve our service", with no further information to supplement this statement. Such vague descriptions are generally not sufficiently transparent, in that they may not enable you to understand what the controller actually does with your personal data.

It is also possible that service providers fail to disclose all of the kinds of processing they undertake in relation to the personal data you provide; don't provide enough detail about secondary purposes like 'research and development'; or fail to adequately describe how and when they share personal data with other 'partners'.

Steps you can take to protect your personal data

You can take steps to try to be informed and to determine that a data controller lives up to their duty to be clear and plain with you. When signing up to an online service where you are providing personal data, or shortly after you sign-up, we recommend that you take the time to read the privacy policy and understand how your data is used by that service. If there is anything that you are uncomfortable with, consider whether you want to use that service or not, or if there are particular features that you may not wish to use because you are not satisfied you understand what processing is going on.

As a general rule of thumb, you should not provide personal data to an online service without knowing how the data will be used. As mentioned above, it is the responsibility of organisations to ensure they provide you with complete, easily accessible and understandable explanations of what they will do with your data. If you want to be cautious, only provide the minimum amount of personal data necessary to use the service you wish to use.

When you sign up to an app you should also try to understand how the data it will collect from you will be processed after you install it. When you use features in an app or service that ask for your personal data, look for and read any pop-up notices or extra information and 'learn more' links. If you are not happy, you may still want to use the service or the feature in question, but you can also follow up with the organisation and ask them questions to explain better what is happening with your data.

Cookies and Tracking

What to be aware of

Organisations that create profiles about your activity online often make use of cookies. These are files that are created in your web browser[2] by organisations when you visit their websites in order to record things about you that can be recognised when you visit

[2] A browser is software tool on your phone or desktop computer that allows you to browse the World Wide Web. Examples of browsers are Google Chrome, Microsoft Edge, Mozilla Firefox, and Apple Safari. There are many other browsers available for use.

again. Generally, you will be prompted in some way to accept them with some description about their purposes.

Cookies can contain records about you like your language preferences on a site or your search or shopping activity and may also contain a unique identifier for you. Information in cookies is transmitted back to the website every time you visit a page, click a link, or interact in any way with the site. The site owner can use this to track your behaviour, infer interests from that behaviour, add this information to a profile they maintain about you, and can sometimes relate what you do on their website to things you do on another website.

So-called third party cookies are created when the website operator allows another organisation to use part of their webpage for things like advertising, social media interaction, weather updates or other widgets.

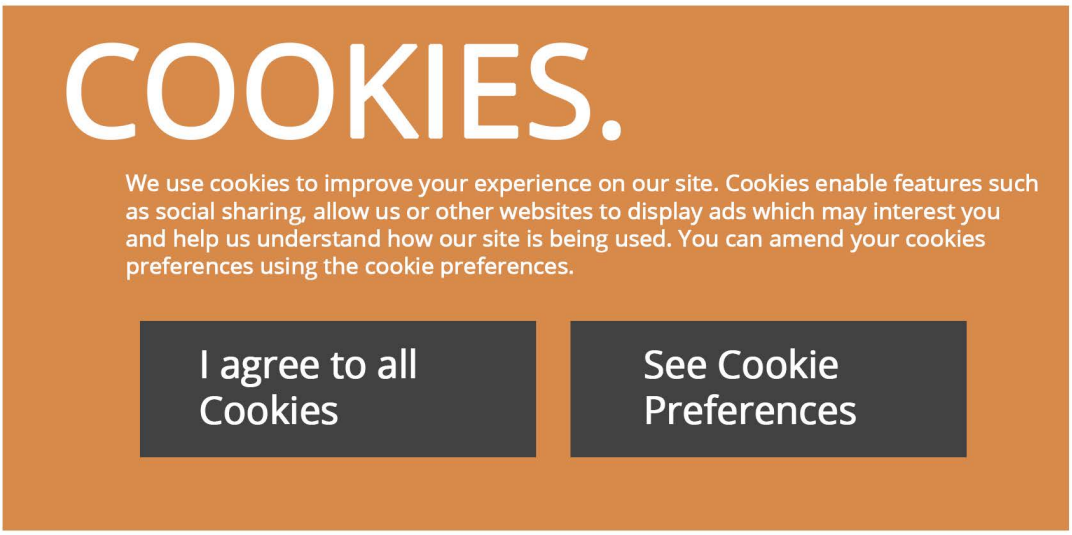
What is the risk to you online?

Tracking your behaviour on websites, and potentially many different organisations exchanging information about your behaviour on different websites, can be very detailed. It can reveal details about your home life, your interests and daily activities. It may also be used in some cases to influence your shopping or other household choices you make, like which insurance you buy, how you think about politics or society, or may even impact on your willingness to share or converse about topics that are important to you.

Sometimes cookies that websites categorise as 'necessary' may not be. In fact, under current laws, cookies that are only strictly necessary to provide you with the service you are seeking do not need your consent. So, for cookies that are not in fact necessary, the website should function even if you *don't* give permission for their use, but you may then find that some of the optional features do not work correctly.

Steps you can take to protect your personal data

Carefully consider the information you are given about the use of cookies on websites you visit and who is asking for your permission to use them. Information supplied to you should be clear and comprehensive. It should clearly and plainly explain which cookies are *strictly necessary* to be used to deliver the service you are asking for in visiting the website, and those which are optional. You can choose to accept them or to later refuse them (either with a facility the website provides for you, or by using technical settings in your web browser to control them if you are happy to do that).



If you find that you don't understand the purposes of the cookies that you are being asked to accept then you might either decide not to visit that website, to accept some of them, or perhaps to delete them after you visit the website. Browser settings can help to control the use or lifetime of cookies. Instructions on how to change browser cookie settings are available on many websites, including in the cookie statement on the Data Protection Commission's website.[3]

There are also add in features called 'plugins' that browsers can use that may help you control what cookies to accept and which to refuse. Some browsers have other features that may help the amount of tracking and profiling that can take place by use of 'incognito mode' or 'private sessions' or 'container tabs'.

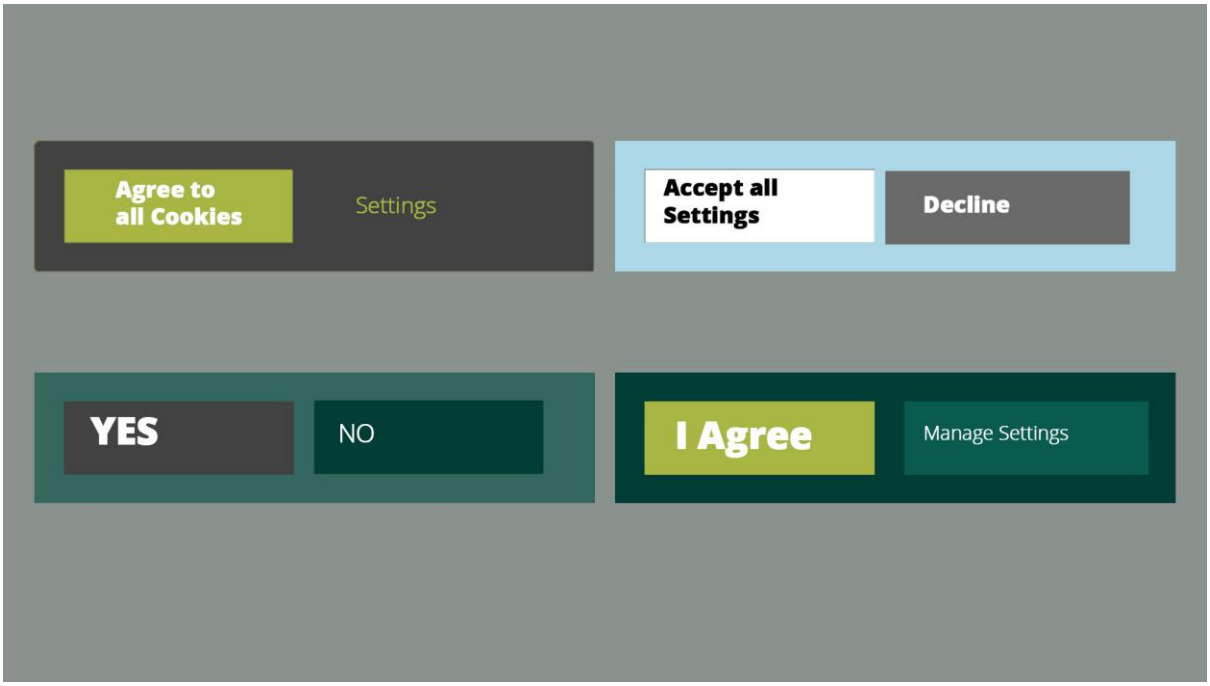
It's important to remember that you may need to do this for each browser, if you use more than one.

Visual Design – 'Nudging'

What to be aware of

Sometimes, when using online services or apps you will come across situations where you need to make a choice about a feature or about the way that the site operator or app developer allows you to use their service. You may need to choose "OK" or "Cancel", "I Agree" or "I Disagree", "Yes" or "No", "Accept" or "Manage Settings".

[3] Please see the section on 'Managing Cookies' at https://dataprotection.ie/en/about-our-site/cookie-policy.



Sometimes these choices can be layered and involve multiple steps. The way these choices and layers are designed and shown to you usually involves a lot of thought and effort by these organisations.

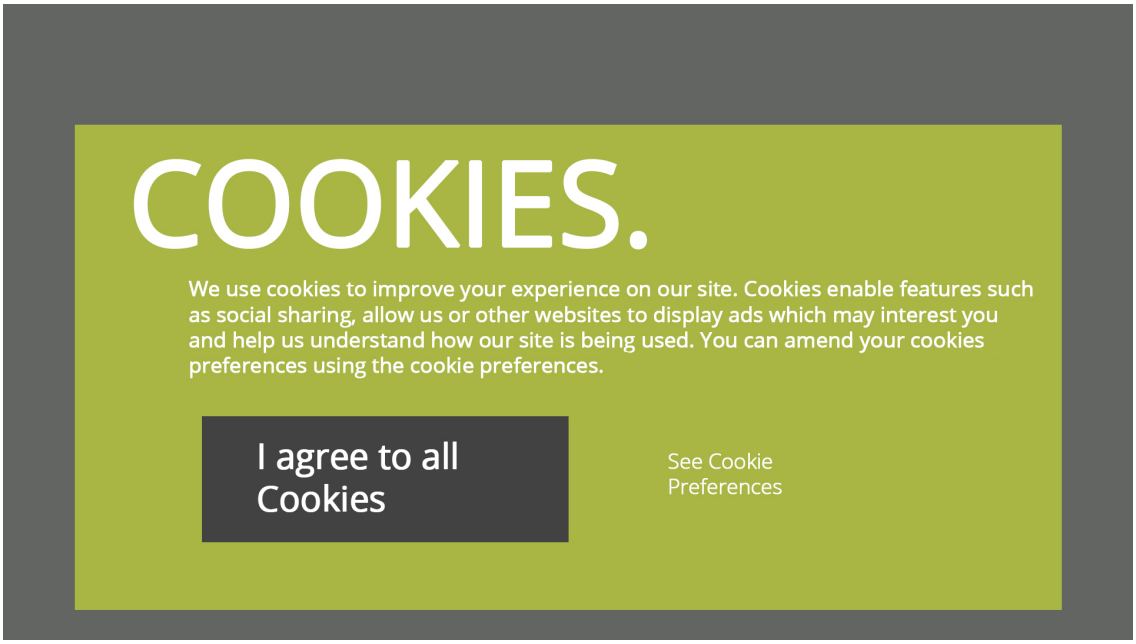
When organisations are designing the way these choices are separated, the way they work, and the way they are presented to you, they should take account of their data protection obligations, including ensuring that information provided is plain and clear and that services should by default only process personal data that are necessary for the intended purpose.

What is the risk to you online?

The design of these controls, and the choices and information you are presented with can be very subtle. For instance, organisations can use branding, colour and font selections to highlight or emphasise certain options rather than others. What you see as the most highlighted choice may not by default be the most privacy friendly choice. Just because an option is highlighted or emphasised using colour or size does not mean that it is the most appropriate choice for users.

For example, you may get the impression at first glance that because the 'OK' button on a screen is coloured rather than grey, or because the 'OK' button is bigger than the 'Cancel' button, that you *should* choose 'OK' to get the best experience. You may be in a hurry and not notice a 'learn more' link nearby or a 'skip' link that may be in grey at the top or the bottom of the screen. In this way, because of visual design and information presentation choices that the website operator or app developer makes, you may be

nudged towards choices that they are most interested in you making, rather than the choice you might have made with clearer information and less nudging.



However, there is a risk that when you choose the most colourful button or follow the steps that are highlighted to you, you may not see or pay attention to the information available, to the alternative choices available, or to seeking more details about what you are being asked to agree to. When this happens, you could end up agreeing to more personal data being collected from you than you expected, or that your data is processed in ways that may not be wholly necessary or even of benefit to you.

There are of course potential issues regarding non-compliance with transparency obligations, or failures to obtain adequately informed consent where controllers have abused these sorts of approaches; however, this note is focused on ways you, the individual, can avoid or minimise online risks as they currently present.

Steps you can take to protect your personal data

We encourage individuals to pay attention to the settings and menus that are presented to you when you use a product or service. Look around the screen you are shown for the other choices that are not highlighted or obvious. Pay attention to the language being used – it may be influencing your choice in a particular direction.

Remember that even if you have a choice to begin with, you do not have to choose anything unless you really want to. You can also consider cancelling or moving back to the previous screen. If there is a 'learn more' or an 'information' button or link, it might

be worth following it to understand more about what you are being asked to do, what the impact of your choice is, and how it benefits you or the organisation you are currently dealing with.

If any setting is confusing or you do not fully understand the control, you should contact the provider of the product or service and seek clarification about the choices you are being offered.

Collection and Tracking

Uninstalling Apps on Mobile Devices

What to be aware of

When your mobile device starts to run out of storage space or when you no longer need an app you might decide to uninstall an app to free up some space. While you may think that doing this means an end to your use of the app and that it and your personal data will be completely deleted by the developer, this may in fact be limited to just removal of the app software from your device.

Depending on the app and the version of the operating system (Android or iOS typically) you are using, there is a good chance that while the app is removed, any personal data that was sent to the developer's servers, including your profile and your account details, will remain on their online service. Generally speaking, removing an app does not also close your account with the app developer or operator.

What is the risk to you online?

When an app is uninstalled and any associated personal data remains on the app developer's online service, this personal data may continue to be processed in ways you do not want and you may still receive messages or notifications from them from time to time. This may happen because the developer cannot tell if the removal of the app from your device also means that you want to close your account.

This means that processing of your personal data may continue, may be occurring invisibly, or without your express knowledge. At the same time, it is possible that the app developer will not remind you that this may happen at the time you uninstall the app on your device. Sometimes there may not be a facility on the devices operating system to notify the app developer when someone uninstalls their app, or the developers may not be using it.

Steps you can take to protect your personal data

When you uninstall an app and you want to stop all processing by the app developer of your personal data you should seek to delete your account before removing the app, or where this can't be easily done, contact them and take steps to close your account. This might be possible by sending an email or by using a form on their website. You will have to identify yourself to the developer to do this so you may need to login to their service, or you may have to use settings in the app before you remove it to let them know you want to close your account.

Apps – Background Processing

What to be aware of

With an increase in more powerful handheld devices, it is now more likely that your mobile device can run many more apps at the same time compared to a mobile device from just a few years ago. Sometimes these apps run in the background – that is they continue to work when you switch to another app to do something else.

For instance, mapping apps sometimes keep track of your location, activity trackers may continue to monitor your heart beat, voice control apps may continue to listen for trigger words like “OK Google” or “Hey Siri”, while other apps may just wait in the background for you to start using them again. Some apps that do this may be collecting excessive information about you, may do so without any real benefit for you, or may do so without reminding you this is happening.

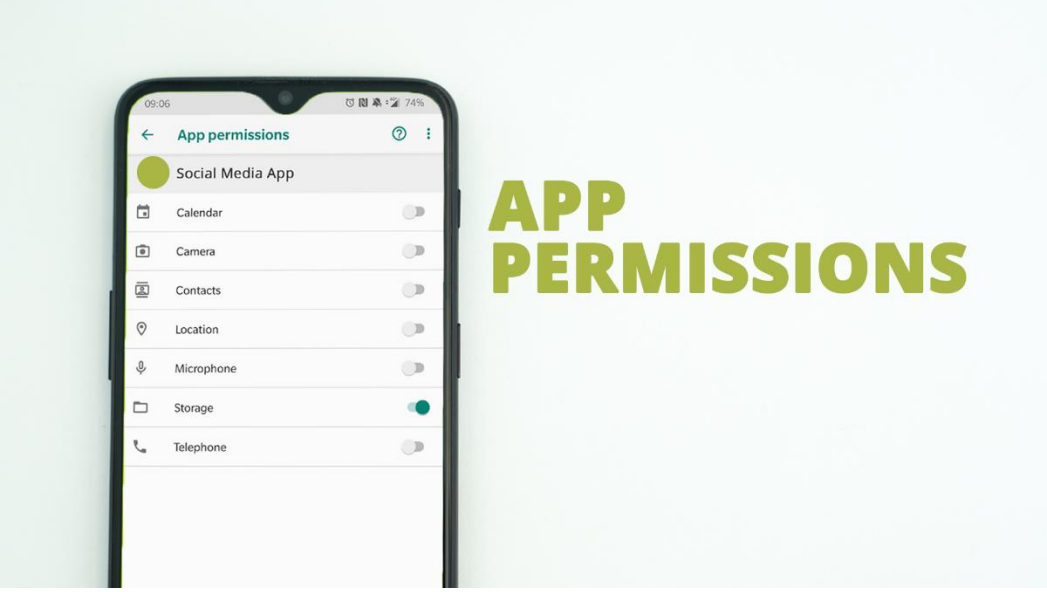
What is the risk to you online?

Apps that are active when they are not being used may continue to process your personal data. Any personal data that is collected may be used to add to a profile being maintained about you and your activities. If this involves personal data like location, heartbeat, or your conversations it could be revealing about your home or private life, and very detailed.

Steps you can take to protect your personal data

Depending on the operating system that you use, some apps that do this allow you to give or revoke permission for this kind of behaviour. You should check for this when you install the app or when considering apps on the app store (look for a link that describes the permissions the app asks for).

After you have installed the app, you can also check in your device settings for the permissions that an app has been granted or will ask for – you can choose not to grant permission if you want. On iOS, you will be notified what permission an app needs when it first needs to run in the background. At this time, you can choose not to grant permission if you wish.



Pay attention to the notifications on your device screen and to the small pictures or icons that appear on the screen – these often indicate background activity that is occurring. You may want to 'pull down' (Android) or 'swipe up' (iOS) on the screen when you see these to be certain you are aware of what is happening. These screens look like those shown below, and will have different contents[4] depending on what is currently running on your phone – like music, location data use, or music player.

[4] Apple list the icons they use in the notification center at https://support.apple.com/egb/HT207354, and Android list them at https://material.io/design/platform-guidance/android-notifications.html. Apps will also provide notifications from time to time telling you what they are doing that you can sometimes also interact with to show you more detailed information.

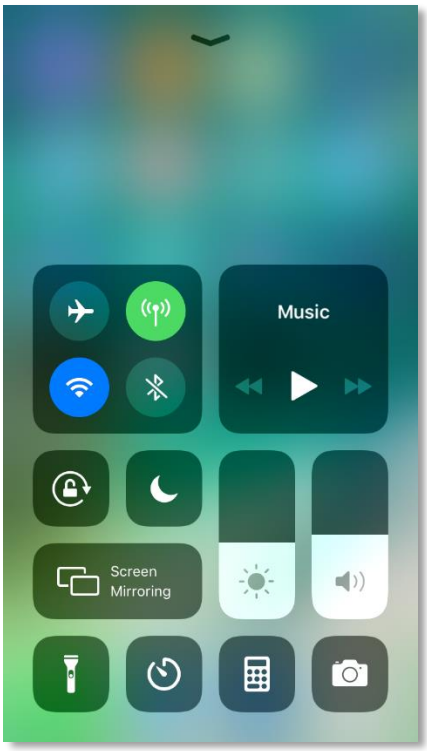


Figure 1 - iOS Notification Center

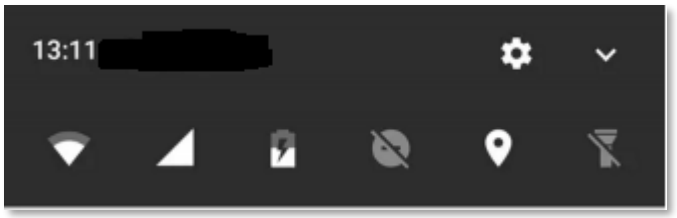


Figure 2 - Android notifications drawer

If you do not want an app to run in the background then you should:

- Exit or quit it where possible.
- Look in the app menu for settings that allows it to run in the background and turn it off.
- In the phone's main settings turn off the permission that allows the app to run in the background.
- Locate the device setting that lists all the apps you have installed and choose the option that allows you to force it to stop (you will have to do this again the next time you use it).

At this point you can also consider removing the app from your device if you are not happy with how it is processing your personal data (see above on uninstalling apps).

Security

Password Reuse

What to be aware of

The use of online services often requires an account to be set up, which is controlled by a username and password for that particular service. Due to the amount of online services available today, many people can have dozens of online accounts, each with a username and password, to keep track of.

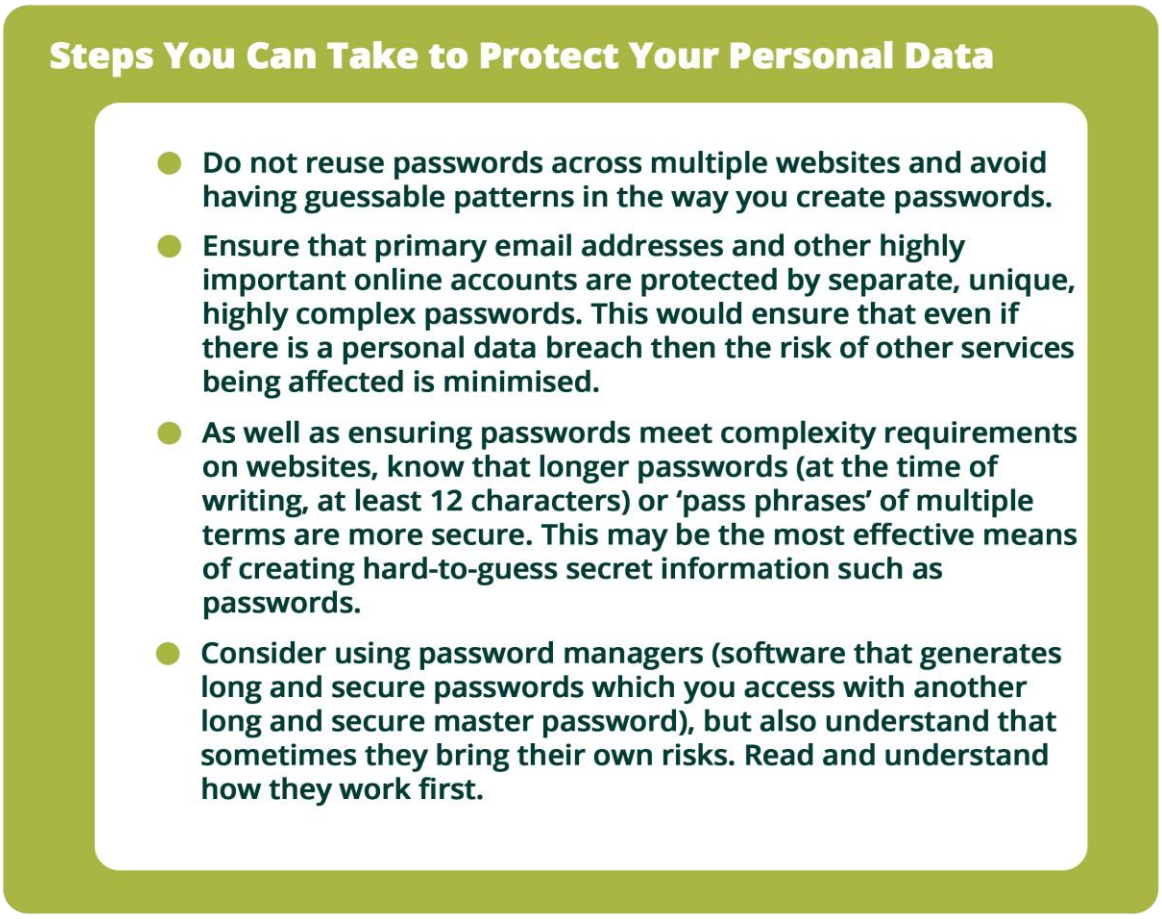
Generally, online services will require that passwords have a certain strength. This means they have qualities that make them difficult to guess or for a computer to attempt to generate. You will sometimes be asked to create passwords that are of a certain length, contain at least one number, use an upper-case letter, or to use special characters. Some services may also require that passwords are updated at regular intervals, say every three months.

Different services can have different strength and update policies. Being asked to update your password can happen at awkward times, or when you need access to something quickly or already have a difficult to guess password. All this can add to the complexity of passwords that a user needs to keep track of and this can be difficult.

What is the risk to you online?

Because of this complexity, re-using existing passwords may become something you end up doing. However, in this case, if there is a data breach that involves a leak of usernames and their associated passwords at a service you have registered with, and where you use the same password for another service, your accounts on those other services may also be at risk of being compromised. Organisations try to protect passwords in this situation by irreversibly scrambling them so they cannot be discovered or guessed, but sometimes the techniques they use may not be enough to prevent them being abused by a hacker.

This would mean that even if the online account that was initially breached was of minor importance to you, if you used the same password for your email account, then that too is at risk. As noted below on ‘Security Questions’, the reuse of passwords may then put other important confidential services you use at risk.

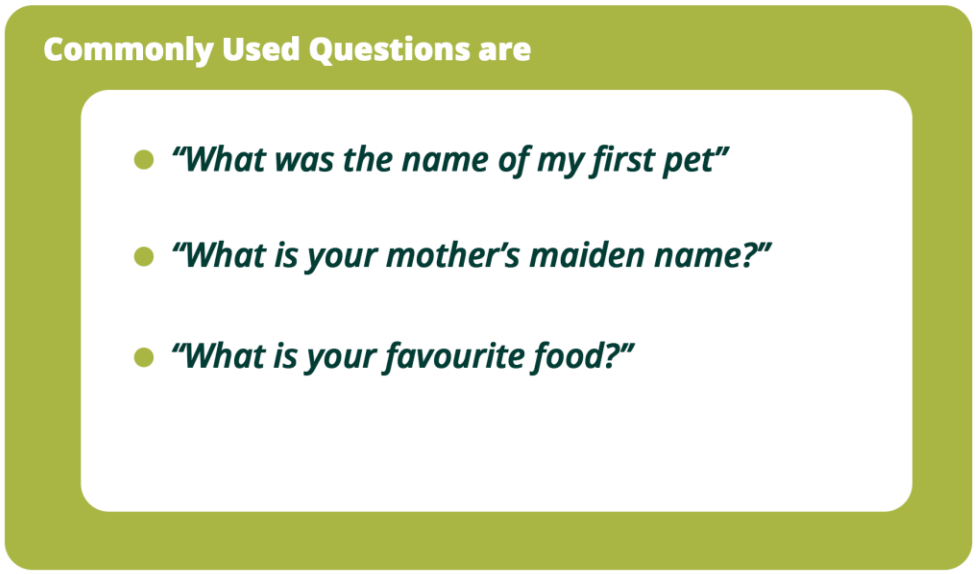


If you are offered a second factor way to verify your identity (often called 'two-factor authentication' or 'multi factor authentication') such as using software to create random codes then we encourage you make use of it. This is discussed some more below on the topic of security questions.

Security Questions

What to be aware of

When creating a user account for online services, users will often be prompted to provide alternative or secondary confidential information to prove their identity in case of a forgotten password. Some services, particularly where customer interaction takes place over the phone, do this by using a set of questions related to you or things that you do or know.



However, these questions can give a false sense of security, or in fact may not be secure. This can happen because the answers may not necessarily be a secret or can be guessed.

What is the risk to you online?

An inherent risk with such secondary questions is that the answers can often be found through research of publicly available information associated with that person, or by personal association with that person. This can happen because, for example, a previous data breach[5] contained answers to some of these questions, because some answers might be available in your social network posts, can be found in a public database somewhere, or can be easily guessed.

The biggest issue arising from another person being able to answer your security questions is that the account associated with those questions could be compromised and taken over. This means that you might lose access to that account when the password is reset by someone else. If it's the case that the compromised account is for the email address or the login name you used for other services like online banking, your health insurance, or pension service, then someone could reset the passwords on those too.

[5] A personal data breach occurs when your personal data is accessed without authority or when it is accidentally or unlawfully lost, destroyed or altered.

Steps you can take to protect your personal data

When setting up an online account, you may be given options to identify yourself in the event of a forgotten password other than by using secondary questions. These rely on you providing extra secret information beyond your password – often a generated random code that is either sent to your phone for one time only, or a code that is generated using a secure app. This is called 'two factor' or 'second factor' authentication. These techniques are regarded as more effective security techniques than secondary security questions because they require the use of a means other than a login password and a personal question to prove your identity.

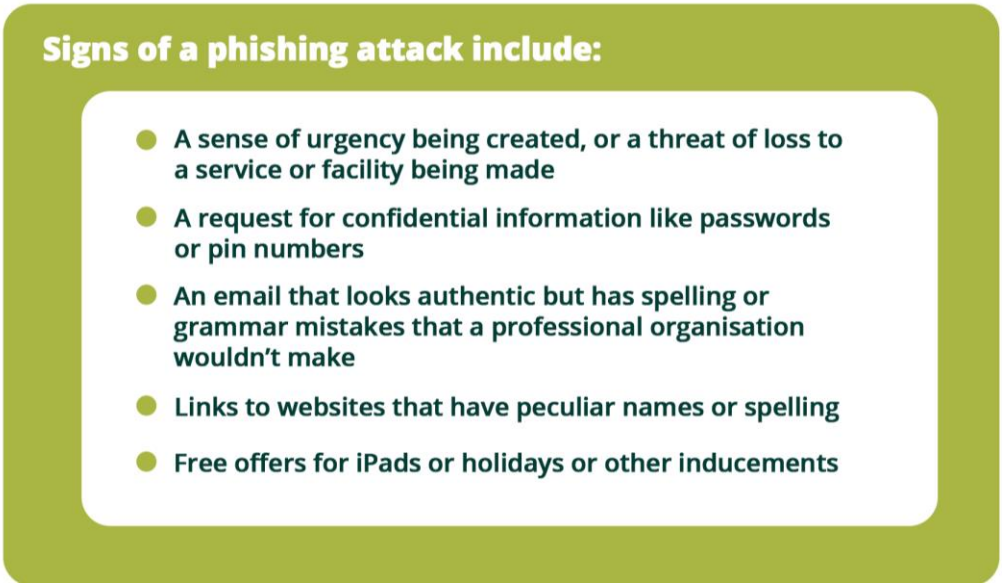
There are many options for second factors for authentication available as alternatives to security questions, such as using an alternative email address as verification, or using an authenticator app, which are often more secure. The data controller decides which they will offer you.

If your only option is to use secret questions, ensure that the answer is only known to you. Alternatively, you could make up answers that you can remember in future and that are not normally associated with you – your favourite food could be something you have never eaten, or perhaps something completely unrelated to food – the idea is that the answer should not be guessable or discoverable. However, if you are offered a more secure second factor means to verify your identity, you may want use it rather than secondary questions.

Phishing

What to be aware of

Phishing is the practice of trying to deceive people to divulge confidential information which is then often used to assist in breaching an organisation's security measures. Phishing may occur using different means but typically occurs through email 'spoofing' – phone calls or messaging applications where an attacker pretends to be someone else or to work for an organisation you know. The attacker persuades you to handover confidential information.



Often phishing attacks are indiscriminately directed towards a large number of users in the hope of a small number of people responding. When hackers specifically target an individual user or a small group of users, this is known as 'spear phishing'.

What is the risk to you online?

Whoever is behind the phishing attempt aims to gain your confidence and make you believe they are genuine and trustworthy.

In doing so, phishing aims to breach the security of a service you use and to steal or extort money or other valuables from you or an organisation you have a relationship with. A phishing attack aims to get you to divulge information that allows an attacker to do this.

In some cases, phishing doesn't ask for information but asks that you install unverified software or apps that are in fact malware or spyware – that in turn collects the confidential information about you that the attacker needs.

Steps you can take to protect your personal data

Phishing attacks can be very sophisticated and underpinned by information that has been found about you from other sources or that an attacker can make a good guess at. The following are some tips for identifying and avoiding phishing attacks:

- ☑ Pay attention to links in emails and on webpages that you connect to. Try hovering over the link before you click it; you should see the destination URL at

in the bottom right of your browser. Is it familiar to you? If not, think again about using it (see also the section below on Fake Sites).

- ☑ Look for spelling errors in the address used in links before you choose to click – https://www.dataprotecton.ie is not the same as http://www.datatprotection.ie or https://www**w**.dataprotection.**com**.
- ☑ You may also check the specific URL using a URL checker tool such a Google safe browsing.
- ☑ Under no circumstance should you ever give PIN numbers or other sensitive information over the phone. No one except you needs to know your password – ever.
- ☑ If a link in an email from your bank asks you to "log in here" to view your account information and you have any doubts, you can always go to your banks website directly to log in, instead of clicking the link in the email.
- ☑ Often website addresses are shortened with what look like codes to hide the true destination of the link. Some online tools[6] can check these for you. You may also want to consider not clicking any shortened website address that you see in any email links.

Unsecured Login Forms

What to be aware of

Web pages that allow processing of personal data over a network should be secured to prevent others listening to or observing (eavesdropping) the information as it moves from your browser or apps to the service you are connecting with. Many people are aware that pages with login forms should be secure – you will see a padlock and the website address begin with "http**s**" rather than "http".

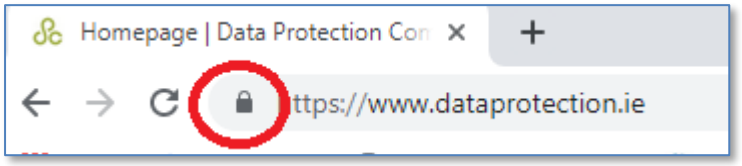


Figure 3 - Secure website indication

This means that your data is encrypted while it is being transmitted, and should then be safe from eavesdropping. Login pages asking for usernames and passwords must be secured this way to encrypt the username and password you enter as it is transmitted to the website or app service that you are using.

[6] For example, http://checkshorturl.com or http://www.getlinkinfo.com.

What is the risk to you online?

Securing web pages may seem like an obvious thing to do, but security measures have to be used comprehensively by online services to be effective, or gaps and weaknesses can arise.

Because unsecure web pages can be manipulated, especially those pages that a site owner does not secure, it may turn out that a login page may not be what you think it is (site owners should instead secure all resources on their website). In such a case a hacker has a technical opportunity to interrupt the flow of information from the page you were on *before* you visit the login page. The result may be that what you are seeing is in fact a fake login page.

With the advent of cheap and sometimes free security certificates that organisations can use with websites, the risk of this arising is when websites and apps are updated frequently or when the organisation designing and updating the app doesn't take an 'all-or-nothing' approach to securing their webpages or their app. However, if and when it does happen it can lead to your login name and password being shared with someone who wants to steal them and take over your account.

Steps you can take to protect your personal data

Pay attention when you visit websites where you have an account that you login to. The website address in your browser should have a padlock symbol beside it. All pages should have this symbol.

If any page on that website does not have a padlock and at any time it asks you to login, be wary of using it.

Some browsers have add-on features or tools called plugins that attempt to make sure that where a website has such an unsecured web page you will be automatically redirected to the alternative secured web page[7].

Domain Names – Spot Fake Sites

What to be aware of

On the web, a website or domain name such as www.dataprotection.ie, www.gov.ie. or edpb.europa.eu is a protected piece of information that an organisation generally must

[7] Some example plugins are called 'Https Everywhere', 'SSL Enforcer', 'Https Now'.

pay for so that no other organisation or person can use it. These are stored in a global system called the Domain Name System (DNS). When an organisation registers the name they have to provide information about their organisation. This can be queried using a tool called WHOIS . For instance, if you search for "WHOIS www.dataprotection.ie" you will see websites that show you details about the Data Protection Commission and who registered the domain name.

What is the risk to you online?

Understanding who or what organisation is behind a website is an important element of online trust.

Website names can be made to look familiar when they are fake. A fake website may have one extra letter in its name, or use a number instead of a similar looking letter (e.g. a number 1 for a letter l), or use an international version of a letter (e.g. an é instead of an e). There are also other technical means or opportunities for hackers to lead you to fake websites, including when websites are not fully secured (see above), or when websites names are not well managed by the operator.

For less popular sites or for websites that you are unfamiliar with, and perhaps ones that ask you for credit card details or to login using your name and password, it may help to check and see if you can find out who owns the site and where they are.

Sometimes WHOIS doesn't have this information but if you are suspicious about a website because you have not used it before or because the domain name looks strange, WHOIS can be a useful tool. If WHOIS doesn't have information on the site owner then it may be that you need to reconsider giving this site or service any personal data.

Steps you can take to protect your personal data

You might consider using WHOIS to get information about a website when you use it for the first time, or for instance if you are about to use your credit card for the first time on a website.

If you see web links in emails, you might use WHOIS to check them. Spam or fake emails sometimes use links to websites that have domain names that look familiar but subtly different – so you might see an email message from www.dataprotection.io, www.guv.ie, or wwww.edpb.europa.eu and take time to think whether it might not be from a legitimate sender. In this case using WHOIS to help understand who the owner of the website in the link is can help you decide if it is fake or is a risk to visit (see also

the section above on Phishing, especially if these links seem very short and seem to use codes instead of names).