Cyber4Dev

CYBER SECURITY AWARENESS TOOLKIT

CYBER4Dev

NI·CO

Republic of Estonia
Information System Authority

Foreign, Commonwealth & Development Office

Ministry of Foreign Affairs of the Netherlands

Funded by the European Union

Introduction to this Toolkit

- **The objective of this toolkit.**

Cybersecurity is rapidly becoming a major challenge that threatens to impact all of us, no matter where we live. With well over half the world's population now online, the Internet is creating a world of opportunities, and providing a range of services, even for those who live in remote communities. But with these opportunities comes risk – especially if we fail to use it safely.

The purpose of the toolkit is to make available a range of materials – presentations, templates and other resources, that can be used by anyone to educate themselves and others about how to stay safe online.

- **Working with the modules – a flexible approach**

The modules are organised under a variety of general categories: youth, general public, organisations. Within these categories, we have developed a few themes: cyber, scams, privacy etc. We also have of module that focus on risks to women, since these are exposed to some specific risks. The modules can be mixed as might be appropriate for the given needs of your target group. However, we would encourage you not to try to squeese too much information into any one presentation as there is a risk of overwhelming the audience. A good rule of thumb is to plan for 60% of the session to be given over to group discussion and exercises.

- **Broader campaigns**

While we understand that many of you may just wish to use some of the presentations here, changing habits is usually a task that requires a sustained effort. It is only when we hear the same message repeated by different people over time in different contexts that most of us begin to take it seriously. That is why we have included a 'Public Awareness campaign' toolkit to help you design a broader campaign. This helps you identify the key outcomes you want to achieve and to profile your target audiences so that you can create messages that you feel they will respond to. An important suggestion is to build coalitions and synergies with other groups to have more impact.

Table of Contents

SCAMS

A guide to spotting scams on the internet and how to reduce the risk of being targeted

Intro

There are more and more scams out there – in some countries 50% of all crimes are enabled by phones and the internet. In 2021, 80% of people online experienced a phishing attack in the US. The alarming thing is, internet scams are no longer so easy to spot.

Scams are constantly evolving and some are becoming more sophisticated. Nowadays hackers and criminals are finding new ways to fool us, like using information we share online to send much more sophisticated messages. The aim of these is to get you to provide personal data, such as passwords, to click on malicious links or to download attachments with malware.

There are several different types of scams. Here is an overview of the most common ones.

Phishing is one of the oldest and most common online threats, yet it continues to be effective. Phishers pretend to be someone trustworthy – a friend, your bank, mobile phone company or a work colleague – in an attempt to get you to hand over information or click a malicious link via email or in apps like WhatsApp.

The SMS message below, purporting to come from the Irish postal service is an example of these. With more and more people ordering things online, the chances that the recipient is expecting a parcel is significant. Such a person might well thing that they had not provided enough for the deliver or customs fee…. And click on the link to make sure they get their parcel.

Spear phishing is a more sophisticated attack that is targeted specifically at the recipient. The message will reference an organisation or person you know or trust, such as your bank, your school, your work place, or a shop that you buy from. Getting an email from someone we know lowers our guard.

Scammers are able to use spear phishing on a mass scale because they use information they can find about us on the internet to send us messages or emails from organisations we interact with. (See Digital footprint module).

To do this, they only need our email address to get started. This is because our email will be linked with most online accounts we've ever set up, such as our Netflix, Amason, Facebook, or even banking accounts. With this information they can launch a targeted phishing attack with the aim to trick us into giving them your banking details and password.

What is a Phishing attack?
These are messages or emails impersonating people or organisations you would trust. The goal of these emails is to get you to provide personal information such as passwords, click on links – for example to a copycat website, or download attachments containing malware.

Example 1. A hacker sends you an email that seems to come from Netflix with a special offer (closing soon) or informing you that your account has been comprised and you need to verify your login details. If you don't have a Netflix account you might ignore it, but they're hoping that 1% of people will respond. This could require you to click on a link that can send you to a fake Netflix website, where they would request you payment details. Or it could download malware onto you device. By providing the information or downloading the document they can access those accounts, steal money, or impersonate you.

Example 2: From your social media accounts they might also be able to find out where you work, what school you attend or who your family and friends are (see out digital footprint module for more on this). With this they can target you with personal information over text message, through a dating site, etc and trick us into downloading malware or handing over personal information.

Example 3: With your email – or a slightly different one, e.g. instead of 'JohnSmith@gmail.com' they might just add a period John.Smith@gmail.com, to set up a very similar email that few will spot. With this they can impersonate you, to scam your friends, employees, colleagues etc. They can also set up fake social media accounts in your name, using your photos.

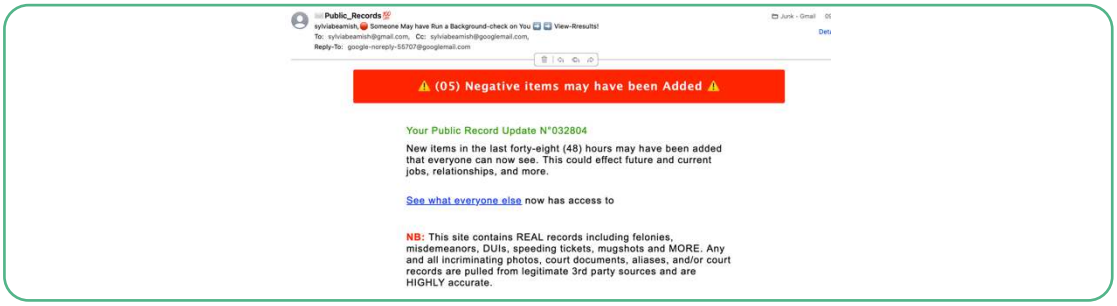
All of this is to say that scams are becoming much harder to spot, and so we must learn to be vigilant. There are a number of common feature to look out for though.

Tips to help spot phishing attacks

Check the email address of the sender to make sure it looks genuine.

For example an email claiming to be from Walmart should come from an email address like the following JohnSmith@walmart.com. A quick look at the email sender will usually just indicate **Walmart**. But by clicking to the right we see the email actually came from a very different email address.

- **Never click on links or download attachments** in response to an email you were not expecting.
- *Be particularly suspicious of*
  - Any message you receive that asks you to **verify your password**, or to update or provide personal information.
  - **Poor grammar or spelling errors**
  - **Unexpected emails or messages suggesting the need to act quickly** to avoid negative consequences or last-minute opportunity to snag a great bargain are a red flag, such as:



- Pop-up ads or emails that sound too good to be true.

REDUCING YOUR RISK OF BEING SCAMMED

But there is also a lot we can do to reduce the risk of being targeted in the first place. For example:

Use strong unique passwords on all your key accounts. This limits the risk to other accounts if one of your accounts has been hacked. If there is a breach of one of the accounts you are registered with – for example LinkedIn - your password for that account will probably end up on the dark web. Hackers check these passwords for associated emails. And if you have reused the same password for a different account, they can break into that account too. For more on creating strong passwords, check out our Cyber security fundamentals module.

Use two factor authentication (2FA) whenever available. More and more accounts are offering or requiring you to set up two factor authentication. This means that when you try to access that account from a new device or different location, or they detect some other suspicious behaviour, you will be sent a code to your phone or secondary email that you will have to enter to access your account. The purpose of this is to verify it really is you trying to get into your account. With 2FA, even if a scammer gets both your email and password, you will receive a code to your phone or app to verify that it really is you. If you receive a code for an account you haven't tried to log into, this means your password has been compromised and you should change it immediately.

Two factor authentication (2FA)
2FA is a code that will be sent to your phone or app that you will need to input if someone tries to access your account from a new device, or is suspicious. In this way, a hacker will not be able to access your account just with your email and password.

Use a password manager to help you remember all your passwords. That way you will not risk forgetting one of your complex passwords as long as you remember your master password.

Check if any of your accounts has been compromised. Check if any of your accounts are no longer safe. Major companies are increasingly being targeted by hackers and data breaches can result in customers personal and financial data being compromised and traded. In 2021, 700 million users' data was stolen when LinkedIn was hacked. And when they succeed, the hackers gets the emails and passwords of all those who have created accounts with them. To learn f your email or phone number has been compromised go to the site 'Have I Have I Been Pwned"

Enter your email address, password or phone number to find out if you have been part of a major hack. If yes, immediately change the password for that account and any others you might have used the same password for.

Make sure any websites you use are secure.

Reliable websites starts with HTTPS, not HTTP. More often you will simply see a padlock at the start of the website.

Make a habit of checking the URL A favourite hacker's trick is to create fake sites that look very similar to the legitimate site. For example, you often buy from a favourite store. Then one day you get a message that looks like it's from that same store with a great bargain. There is a link to order your offer. But when you click on the link instead of going to the real site, you get one that looks the same but which has a slightly different 'url'. This one is controlled by a hacker; some of these are very convincing. So if you enter password details or bank account details, bingo, the hacker has your details.

For example, which of the following is likely to be a fake site

- www.Amason.com
- www.Amason.co.uk
- Amas0n.com
- Amason1.com

Use a secondary email when creating any non-key accounts Most of us register with tens of accounts over time. With each of these we enter our email and a password. Often times the same password for many accounts. If instead of using our primary account for most of these we use a secondary email, our main personal email will not be compromised if those accounts experience a data breach. You are also less likely to receive as many spams emails, since owners of accounts you sign up with typically 'track your cookies' – and resell your data.

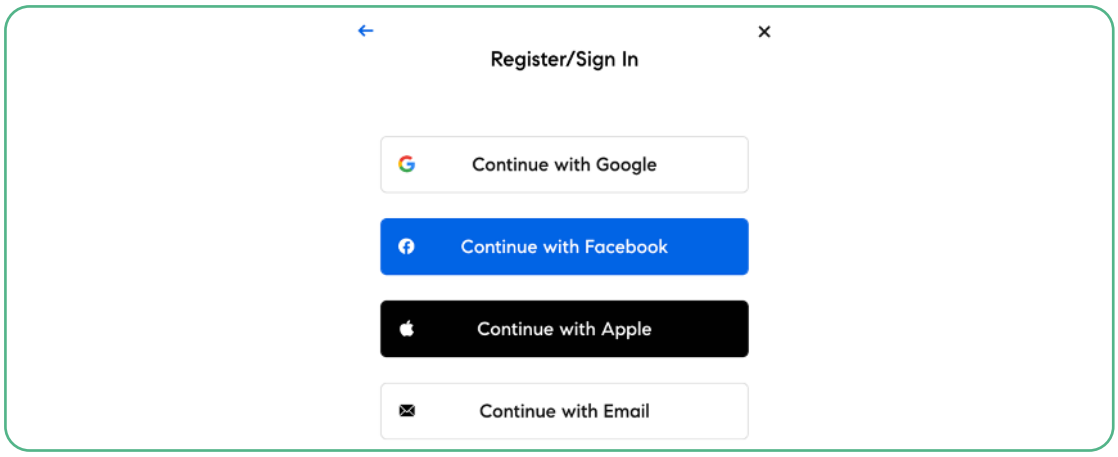
Example: You want to buy a concert ticket online. If it's your first time on this site, you'll be asked to create an account and for this you'll be asked to provide an email address. However, you don't have to provide your primary address. If you create a secondary account this will reduce the number of ads and phishing attempts you are likely to get.

Don't let websites save your payment details

When shopping online, the websites you visit will automatically offer to save your card details. If this is a place you might want to buy from regularly, it may be very tempting to click the 'Save card details' options so that you don't have to enter your payment details each time. However, saving your bank account makes you vulnerable if that site is ever hacked. It is much safer to live with the inconvenience of entering the details each time.

Don't Login With Facebook or Google

Often instead of using an email or password to access an account, you will be given the opportunity to log into an account via Facebook or Google. This may seem much easier than registering your email again with yet another service provider, but most people will have a lot of personal information on Facebook. And when you log into an account using Facebook, the account you are trying to access will get access to all your information and can be shared with third parties.



Always update your software, especially anti-virus.

When prompted to update your software, do so immediately. Most software updates provide patches for vulnerabilities that have been discovered. Outdated software can give hackers a backdoor for accessing your private information. So update your software when prompted. And don't assume it will update automatically overnight if set to do so. Because this won't happen if you don't switch off your device.

OTHER COMMON SCAMS

Copycat government websites. Especially since Covid, when many services went online to enable people to stay home, and governments offered special financial support, copycat government websites have been set up to offer government services or financial support. These then collect data, including bank accounts.

Work from home fraud. You are offered a chance to earn money working from home, but first you must pay a fee, for example for business leads.

Unexpected windfalls... that require you to pay a small fee. You are notified that you have won the lottery, or have received an inheritance, or even a parcel. But first you must pay an admin fee, or a customs fee. The promise of getting a lot more by paying a small amount can be very tempted.

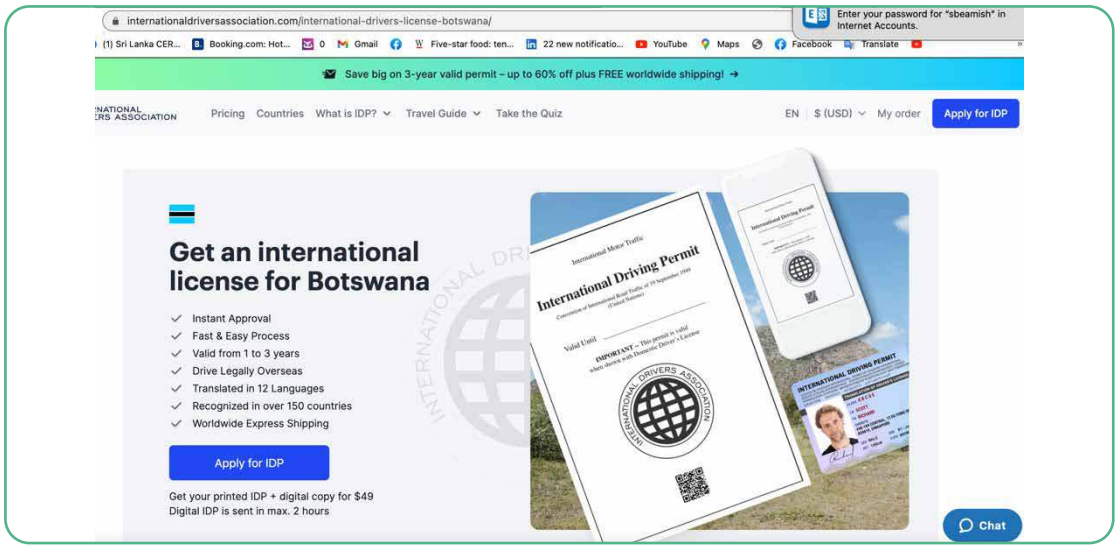
EXERCISE

One of the most common scams are copycat government websites. Here's an example.

Copycat government websites. You go to renew your driving licence online. You click open the first website that suggests it can help you process this application. The following website pops up.

Question: The site looks official, but how do you check that the site is legitimate?

Copycat government websites are a very common scam.
They will typically charge a fee for services they may not even be eligible to provide. They may also steal your data.

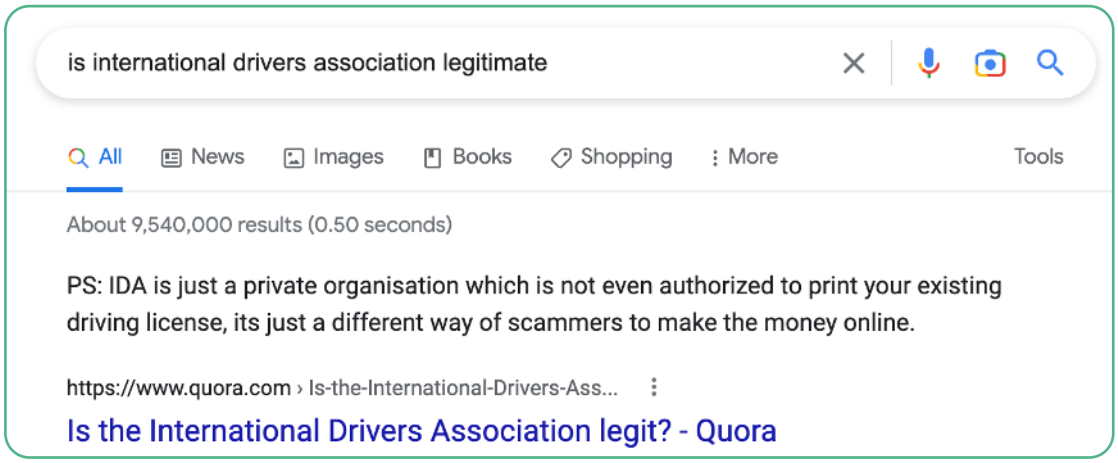


The first thing to do is to check the URL. Official documents will almost always be issued by government websites. If you google a government ministry in Botswana, such as the ministry of Finance, you will see that the URL ends in 'gov.bw'. Thus that is part of the URL for all government sites.

(Also, when you look up an official site the Wikipedia summary will appear on the right.)

Since the International driver's association is clearly not a government site, further research is recommended.

If you google the international drivers association you will get the following warning.



Lessons learned

- Check the URL very carefully
- Google the organisation to check if the URL looks right or the organisation seem legitimate.

Exercise 2. Checking out a legitimate URL

Which of the following looks legitimate?

www.cnnofficial.com

www.cnn.com.co

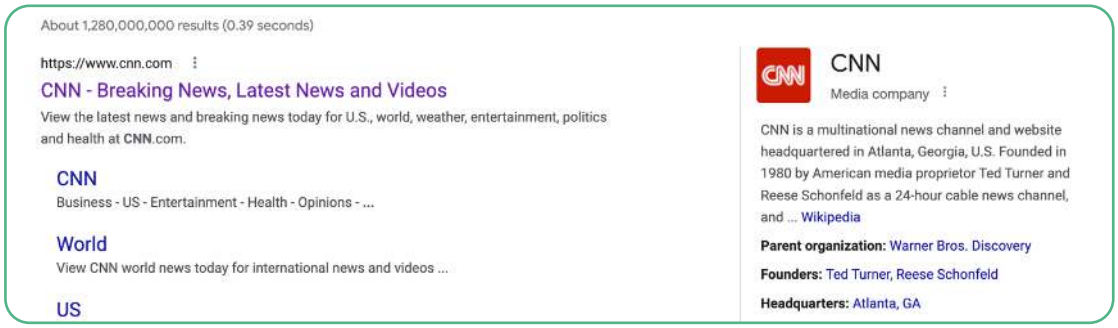
www.cnn1.site/business.news

www.cnm.com

http://google.com

http://google.net

Typical modifications will involve a typo, an extra number. If you're not sure what the correct URL is, google the organisation. This confirms that you should see https://www.cnn.com. Also note that the summary of the site is displayed on the right.



Digital footprint

How and why we should protect our online privacy

What is a digital footprint?

Our digital footprint is the trail of data that we leave behind when we go on the internet. This includes emails, social media, where we shop, what we buy and forms we fill in. All this builds a picture of us.

Why does this matter?

Whilst it should not stop us going online, a digital footprint can be used in ways we don't expect:

- They are relatively permanent – so something we do online aged 16 can affect us years later.
- A digital footprint can determine a person's digital reputation, which is often as important as their offline reputation. Employers can check their potential employees' social media profiles, before making hiring decisions.
- We have little control over our words and photos once they're posted online. They can be misinterpreted or taken out of context, leading to embarrassment or insult.
- Cyberbullies can alter their victims' photos and share them across the world.
- Cybercriminals can exploit your digital footprint to conduct phishing scams, blackmail or create false identities based on your data.

- Companies that run websites and apps often treat our data as a commodity that can be sold or exploited.

Two ways we build a digital footprint

There are two ways we share our data:

- Actively, and
- Passively

Our **active digital footprint** is when we deliberately shared information about themselves. This includes posting on social media, buying from a website or completing an online form.

A **passive** digital footprint is when information is collected about the user without them being aware of it, such as websites collecting information about how many times users visit, where they come from, what they are looking for or download, and their IP address. This is a hidden process, which users may not realise is taking place. it happens when we go on websites and are asked to accept cookies and we click yes.

Active footprint	Passive footprint
Our active footprint is the information we share online about ourselves (or friends, colleagues etc share, naming us.)	Our passive footprint happens we visit a website and click 'Accept cookies' to access their content.
Collectively builds an image that is worth thinking about since it influences perceptions of us	The site owner collects and then sells information about what we are doing on the site to third parties
Easy for anyone to see, including future employers, immigration officers, in-laws etc.	Usually bought by advertisers to enable them to better target their products or services.
Sometimes the active footprint is created by others with the intention to harass (See our cyberbullying module)	BUT it will increase the amount of spam calls and phishing attempts
Can cause real harm if negative content is not removed quickly.	No guarantee as to who will collect the information and for what purpose (See our module on spams for more

TIPS TO INCREASE YOUR PRIVACY

1. Look yourself up

First and foremost, keep a regular eye on your online profile. It is always a good idea to find out what information a hacker might find simply by searching for your name. If you have a common name you might need to add additional information to find yourself, such as where you live or your occupation. Check different search sites (Google, Bing and social media) since they can provide different results. Make a note of any items that you'd rather not see there.

Where can I see what Google knows about me?

- Go to your Google Account.
- Select Privacy and personalisation.
- Under this Data & privacy page you'll find History Settings, Ad Settings, and more.
- For example, go to Ad Settings and click on Ad Personalization.
- Now you'll see How your ads are personalized.

Aug 30, 2022

2. Delete unflattering or negative content

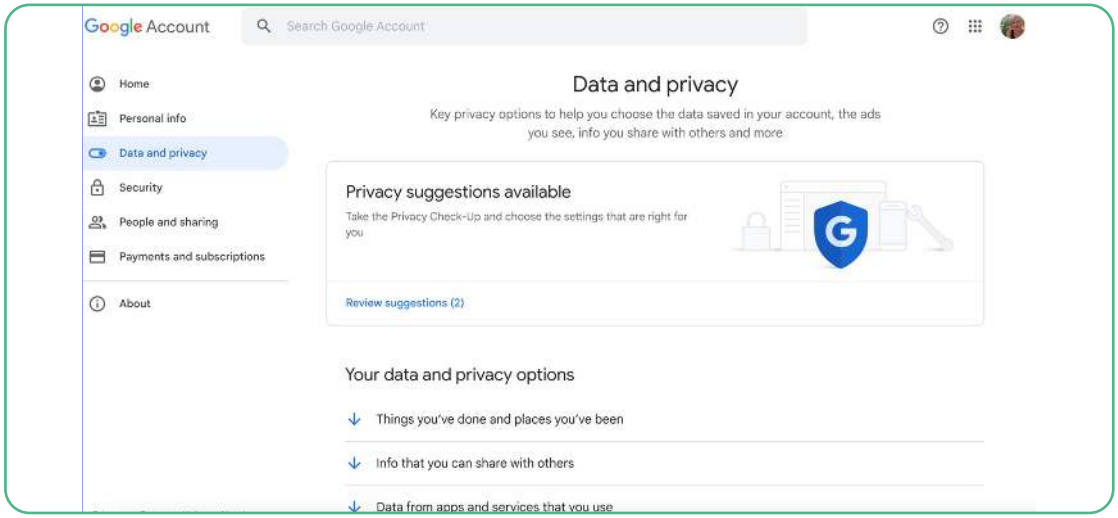
Go through all your social media posts and delete content that you find unflattering, or even that you would prefer not to have out there. If others have tagged you in an unflattering photo, ask them to delete it, or at least untag yourself. For content that is posted on a website, you would have to get in touch with the website owner to have it deleted. If it still shows up in an online search after you've requested deleting the content, you can fill out Google's URL Removal tool to have the issue fixed.

3. Delete old accounts

Over the years, we often change social media accounts, old emails and logins, or we no longer go to the same online stores. Review your devices and delete any old account or apps you no longer use. In this way you reduce the amount of information that hackers can find about you online. You also reduce the risk of having your personal information exposed in a data breach.

4. Update your privacy settings

Scammers can use information such as date of birth, mother's maiden name, pets' names, places you've lived to impersonate you. If you must share information, make sure it is with friends only. So set privacy settings on your social media accounts so that only friends can see your posts and you can see who is tagging to your timeline.



If you check up your google account, the site will provide you with recommendations to help keep your data secure. Your social media platforms will also provide advice to help keep you safe online.

5. Don't overshare.

Sensitive information you should try to avoid sharing online includes your phone number, pets names, your mother's maiden name date of birth, where you live, employer etc. These can often help people guess your password or provide information that a hacker could use to send a target phishing attack. (See our module on Spotting Scams for more on this.) Be particularly careful about sharing barcodes. Sharing a photo of yourself on social media with a flight ticket on which the barcode visible, for example, can provide hackers with your name, bank account details, credit card details, email etc.

6. Be a little careful about opinions you share online.

Remember what you share online, even with friends. Anything that goes online can stay online a long time. And even if your friend can be trusted not to share it more widely, one day that friend's account might one day be hacked. (See also our 'online bullying module for more detailed advice about sharing intimate photos and messages in particular)

7. Learn to use the private or Incognito mode.

When browsing in regular mode the websites you visit will track you by checking what cookies are stored on your computer. But most browsers provide the possibility to visit websites anonymously or 'incognito'. Google how to switch on incognito mode for your browser and use it when you don't want your online behaviour tracked.

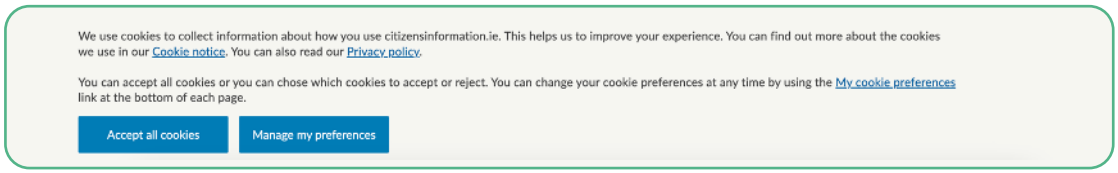
8. Regularly delete your browsing history

Get in the habit of deleting your browsing history. This is especially important if you use a public computer, such as in a library where others will be able to see what you have been browsing. However, even on your own device, your history will store private data required by sites you've visited

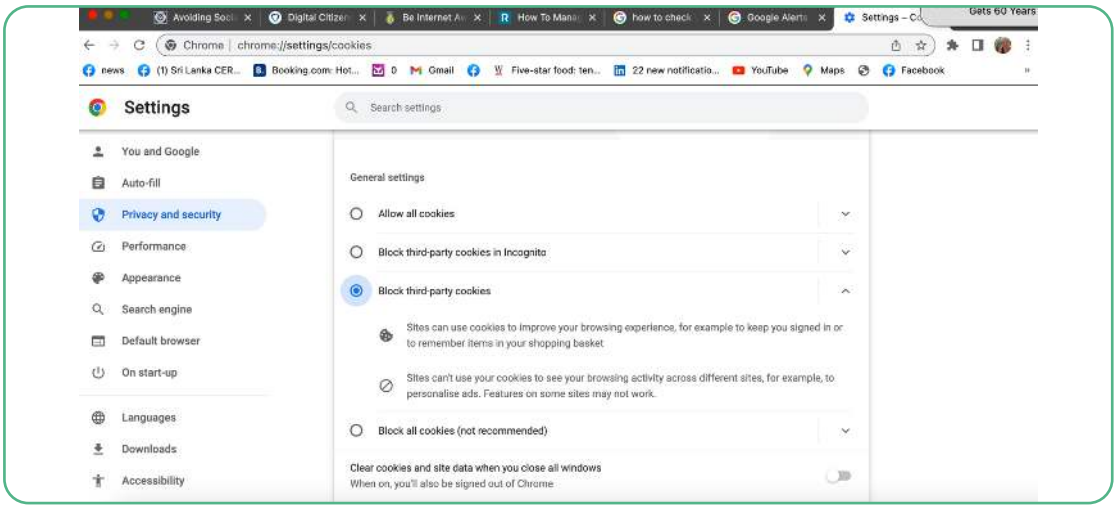
9. Manage cookie collection

Even if you don't go incognito, When you go on a site that asks you to 'Accept cookies' before they let you see their content, click instead 'manage cookies'. Now save the option: "essential cookies only".

Delete your browsing history. When asked to 'accept cookies', click instead.



Set your cookie preferences to block third-party cookies.



Your browser will offer a range of options to improve your privacy. Check out the privacy and security settings

10. Consider installing a Virtual Private Network (VPN)

These are particularly useful when you are on the move and using public wifi which might not be very secure. A VPN will mask your IP address so you can keep your location, browsing history, and other information private.

You should research credible options that might even be available free of charge

11. Encrypt messages

You can increase your privacy by using message-encrypting apps. When you do this anyone who tries to intercept your messages will not be able to encode what is being sent.

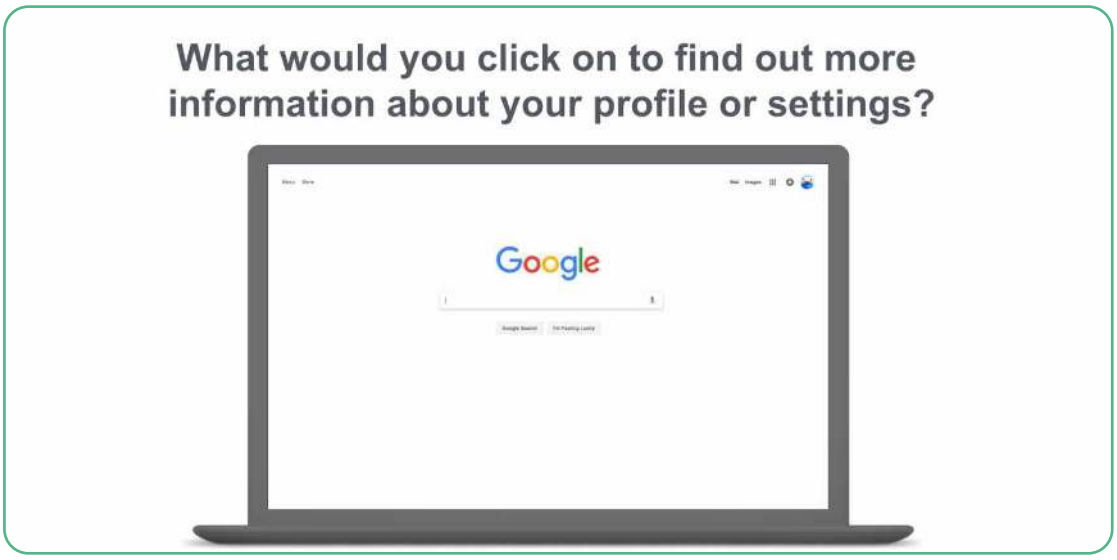
Examples of end-to-end encrypted messaging platforms are Signal and WhatsApp. These automatically encrypt messages (including photos and videos) plus voice calls and video calls so that if a hacker tries to intercept them they will not be able to understand the message. Both platforms also let you use set your messages to disappear on the other person's device after it is seen, and do not permit screenshots to be saved.

12. Log out of your accounts

Make sure you log out of any accounts you maybe have accessed on a public device. Otherwise the person who goes on it after you will be able to access any accounts that might still be open such as your email or social media accounts.

Privacy settings

What would you click on to find your profile or privacy settings?



- Where would you go to change your google account password?
- Where would you go to change your Instagram password?

Which of the following would you want to keep private?

- Birthday
- Contact details
- Places you've lived
- Schools or workplace
- Education or schools

Discussion

Which of these should not be shared on the internet and why?

- Your home address
- Your school
- Photos you wouldn't want your teachers, employers to see
- Information about a public figure (politician/influencer/actor)
- Your best friend's secret crush
- A flight ticket
- A concert ticket that has a barcode
- Photos of you at your favourite hang-out

Which of the following do you think are the two most commonly used passwords?

Password

- 123456
- Ice-cream
- Let'sGoBr@nd0n!

Weak passwords are common or easy to guess passwords,

Exercise

- Write the elements of a strong password
- When is it important to have a strong password
- Make three practice passwords that pass the super strong test.

Which of the following types of cookies can you opt out of accepting?

Cyberbullying – what is it and what does it look like?

Cyberbullying, also known as online bullying, is a form of harassment or intimidation that takes place over digital platforms, such as social media, websites, forums, email, text messages, or any other online communication channels. It involves using digital technology to deliberately and repeatedly target individuals or groups with harmful, offensive, or threatening behaviour.

Cyberbullying can take various forms, including:

Harassment: Sending hurtful, offensive, or threatening messages, comments, or emails with the intention of causing emotional distress.

Impersonation: Creating fake profiles or accounts to impersonate someone and post false or damaging information about them.

Exclusion: Intentionally leaving someone out of online groups, conversations, or events to make them feel isolated.

Flaming: Engaging in online arguments, often using strong language or insults to provoke and upset others.

Doxing: Sharing personal or private information about an individual without their consent, often leading to privacy invasion and potential harm.

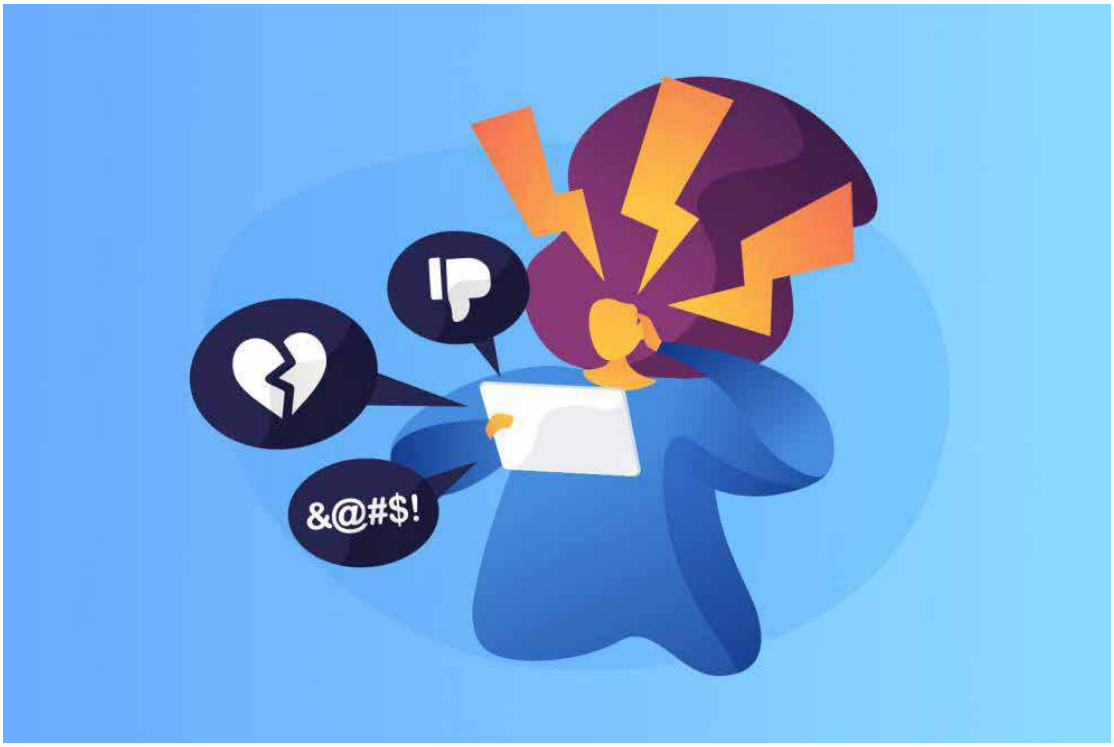
Outing: Revealing someone's private or sensitive information, such as secrets, embarrassing details, or personal photos, without their permission.

Cyberstalking: Engaging in persistent, unwanted online attention and monitoring, often with the goal of causing fear or distress.

Trolling: Posting deliberately inflammatory or offensive content to provoke reactions and disrupt online discussions.

The impact of cyberbullying can be severe, leading to emotional distress, anxiety, depression, self-esteem issues, and in extreme cases, even suicide. Due to the potentially anonymous nature of the internet, cyberbullying can be more difficult to trace and prevent than traditional forms of bullying. However, many jurisdictions have started implementing laws and regulations to address cyberbullying and protect individuals from its harmful effects.

It's important to raise awareness about cyberbullying, educate people about online etiquette and responsible internet behaviour, and create a supportive environment where victims can seek help and take necessary actions to address the issue.



How can cyber bullying be prevented?

Preventing cyberbullying requires a combination of strategies involving individuals, parents, educators, and online platforms. Here are some steps that can be taken to prevent cyberbullying:

Education and Awareness:

Educate individuals, especially children and teenagers, about the consequences of cyberbullying, both for the victim and the perpetrator.

Raise awareness about the importance of respectful online behaviour and the potential harm caused by hurtful comments or actions.

Promote Digital Citizenship:

Teach digital etiquette and responsible online behaviour, emphasizing empathy, kindness, and respect for others.

Encourage individuals to think before posting or sharing anything online and to consider the impact of their words and actions.

Open Communication:

Create an open and supportive environment where children and teenagers feel comfortable discussing their online experiences with parents, guardians, or educators.

Encourage them to report any instances of cyberbullying they encounter or witness.

Parental Involvement:

Parents should be actively involved in their children's online activities, understanding the platforms they use and the friends they interact with. Set guidelines and rules for online usage, including appropriate times to use devices and the importance of privacy settings.

School Involvement:

Schools should implement anti-cyberbullying policies and educate students about the school's stance on such behaviour. Provide resources for students, parents, and teachers to recognise, report, and prevent cyberbullying.

Online Platform Responsibility:

Social media platforms, websites, and apps should have clear and enforced community guidelines that prohibit cyberbullying and harassment. Implement reporting mechanisms that allow users to easily report instances of cyberbullying, and take appropriate actions against offenders.

Privacy Settings and Security:

Encourage individuals to regularly review and adjust their privacy settings to control who can see their online content. Teach individuals about the importance of strong passwords and two-factor authentication to protect their accounts from hacking.

Empower Bystanders:

Encourage bystanders to speak out against cyberbullying and support the victim. Their intervention can make a significant difference.

Support for Victims:

Offer resources and support for victims of cyberbullying, including counseling and guidance on how to cope with the emotional impact.

Legal Consequences:

Ensure that there are legal consequences for cyberbullying behaviours, especially in cases where the behaviour involves threats, harassment, or other criminal activities.

Collaboration:

Work together as a community, involving parents, educators, law enforcement, and online platforms, to address cyberbullying effectively.

Preventing cyberbullying requires a holistic approach that focuses on education, awareness, responsible online behaviour, and support for both victims and potential perpetrators. It's important to create a culture of respect and empathy in both online and offline interactions.

Building a cyber awareness campaign.

Communicating messages effectively to the public or to specific audiences can be challenging.

Information overload is a feature of the modern world and messages on niche or technical subjects can often be filtered out. As the world's global digital footprint expands, it is now even more important to ensure that all aspects of society are aware of potential risks and how to mitigate them.

Effective communication and awareness strategies require consistent messaging over time, ideally being delivered through different sources (national broadcasting, social media, education, business and civil society). These are best delivered through communications campaigns.

Whilst every campaign will be different (where is it happening, who is the audience, what tone you want to strike), planning a campaign using proper sequencing will make your campaign more effective. The materials in this toolkit will enable you plan a campaign suitable to your budget, the people you have available, and local context. These should be seen as tools to support your own experience and training. Some of the toolkits may not be relevant to your campaign planning, so take the ones that will be most useful to you.

> A campaign can be small, or large. It can last a week or a year. But campaigns should always be a series of planned activities over a period of time. Ideally a campaign should involve a number of types of activities.

Below is a brief overview of what is entailed in designing a campaign. We have also developed a slide deck you can use to work through the campaign design with your key stakeholders. By involving partners in the campaign design, they will feel much more ownership and commitment to playing their part. Finally, there is an exercise handout provided (link to exercise handout) to facilitate the group work during your workshop.

Step 1. Identify the issue your campaign will address.

- What problem is your community experiencing online that you think could be helped through an awareness campaign? For example, are a lot of people being scammed? Are the teenagers being cyberbullied? Is there a lot of identity theft happening? It is advisable to focus your campaign on one issue at a time. Otherwise there is a risk you will confuse or overwhelm your audience.
- Once you have defined the issue you will focus on, a brief analysis of the problem might provide some insights. Don't assume you know why people are falling for the scams, being hacked etc. Try to find out as much as you can about how and why the issue is happening. Then ask yourself if they could be helped through awareness? What information or skills would they need to keep them safe? How could you provide them with this information? Would it be easy or difficult to get your audience to accept your message? Who might they listen to or be influenced by?

All this information will be very useful to have before you start to design your campaign.

Step 2. Establish your campaign objectives

Once you have established what issue to focus on, the next step will be about identifying a manageable number of objectives.

In the case of a communication campaign this will involve.

Objectives are often confused with tactics.

"We will raise awareness about the importance of online privacy by 30% in our local schools by December 2023" is a measurable objective.

"We will implement a social media campaign" is an tactic you are hoping will help you achieve your objective. The tactics come in step 5 of your campaign design.

- A change in awareness
- A change in mindset and/or
- A change in behaviour.

The easiest of these to achieve is a change in awareness. Changing a mindset will be more challenging since it involves an element of persuasion. But the most challenging of all will be trying to achieve a change in behaviour. That is because habits tend to slip. Moreover, in the case of cyber security, reinforcement happens only in the negative. If you are successful, nothing happens. Without continuous reinforcement of the message of the need for vigilance, it can be easy to get careless.

Step 3. Define your target groups and target group objectives

There are two important categories of audience you want to reach:

1. Your final audience and
2. Your influencers or mediators.

Your final audience break down into a number of sub categories that are sufficiently different in their profile to justify slight different in approaches. For example a campaign against cyberbullying might involve raising awareness amongst

- Teenagers
- Parents
- Pre-teens

You separate these out, in part because you will reach them through different activities, but also the focus of your messages might be different.

Influencers or mediators

These are the groups that your final target group listen to and are influenced by. Who these are will depend on your audience but in the above example those you might count could include

- Youth leaders
- Teachers
- Sports personalities, etc.

Your objectives for each will be different. For the final audiences you will want them to listen to and accept your messages. For the influencers or mediators, you want them to share your messages.

Step 4. Decide your messages

Once you have decided what you want to achieve and who you are talking to, the next step will be to decide what to say. Cyber security can be confusing – and **overwhelming.**

So you need to decide what do you need your audience to know. How much information

will they need to be able to understand the risks and how to avoid them?

Bear in mind that people respond best to stories they can identify with. The teenager who hears of a challenge another young person faced will identify with (and remember) that story more easily than they will to an instruction or tip. Thus, it is always a good idea to portray real situations and then give tips on how to avoid them. That will always be more effective than a list of tips.

Don't be tempted to give them too many messages.

Step 5. Tools and activities

Consider how we begin to take information more seriously. If you hear a message from one source, you might momentarily notice it, but forget it a day or two later. However, if you see a message online, then hear the same message on the radio, then again from your teacher or your friends, you begin to pay more attention.

The optimal campaign will involve a number of activities for your messages to be absorbed. Social media is good for getting attention. Posters may remind people of key points. But to get people to change their behaviour it is important to engage your audience. Presentations are a great way to make sure people are understanding what you are saying and applying it to their lives. But make sure you include exercises and discussion so that you can gauge what they are understanding.

In this toolkit we have included a number of slide decks. Please note that we have tried to break each down into a single focus. In some cases there might be overlaps. On the issue of cyberbullying we have one slide deck for teens, and a separate one on sexting. That is because sexting involves girls disproportionately, and a separate presentation to girls on this topic might be effective. However, you might also want to use some of those messages for a mixed gender presentation

Do also feel free to adjust the slide deck to your needs. If you have local statistics, new tips, please fell free to use them. If you want to add your logos or different images, ditto. The slide decks are means to serve as aids.

Step 6. Resources and budget

When developing a campaign it can be easy to be inspired by campaigns you have seen. However, these might involve a more significant budget than you might be able to obtain. Don't be discouraged however, If you don't have a big budget, you can still achieve a lot. A presentation in a local school, or library can be done quite cheaply or free of change, especially if you partner with ministries, local municipalities etc. In this day and age of tik-tok videos, social media content can be developed very cheaply.

Step 7. Monitoring and evaluation.

Monitoring and evaluation is a great way of assessing the impact of your campaign. Being able to demonstrate that your campaign has had an effect is also a great way to getting more support for future campaigns. When monitoring a campaign pay attention to the difference between monitoring the success of specific activities – outcome, and that of the campaign overall – impact.

For example, a social media campaign can be measured by the number of likes, shares and positive comments you receive.

Measuring impact will involve trying to establish whether your audience has listened to your message and adjusted their behaviours accordingly. Remember, people might like a social media post, but forget about it soon after. For more on this, check out our monitoring and evaluation.

CYBER4Dev

NI·CO

Republic of Estonia
Information System Authority

Foreign, Commonwealth & Development Office

Ministry of Foreign Affairs of the Netherlands

Funded by the European Union