PROPHETS

Preventing **R**adicalisation **O**nline through the **P**roliferation of **H**armonised **T**oolkit**S**

Information leaflet

Security on the Internet

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786894.

Berlin, April 2021

Freie Universität Berlin (FUB)

Developmental Science and Applied Developmental Psychology
Head: Univ. Prof. Dr. Herbert Scheithauer
Habelschwerdter Allee 45
14195 Berlin
Email: entwicklung@zedat.fu-berlin.de
Homepage: www.developmental-science.de

Project PROPHETS

Coordinator: Dr. Holger Nitsch
University of Applied Sciences for Public Service in Bavaria (BayHföD)
Department of Policing
Fürstenfelder Str. 29
82256 Fürstenfeldbruck
Germany
Email: prophets@pol.hfoed.bayern.de
Homepage: www.prophets-h2020.eu

Authors: Kristin Göbel, Antonia Schendel, Sven-Eric Fikenscher, Herbert Scheithauer, Katie Bailey
Layout: Jenny Köhler
Photo credit: istockphoto

Freie Universität Berlin

The cyberspace is increasingly used as a medium to motivate others to commit terrorist attacks, to finance terrorist endeavours, to recruit and to train individuals and/or groups for terrorist purposes, and to agitate against European social and democratic ideals and minorities.

It has been shown that adolescents and young adults are particularly at risk of being confronted with radical groups and content on the Internet. The phase of searching for identity is a time in which the openness to new content, the search for orientation and curiosity is greater. Unfortunately, this is exactly what radical groups often try to exploit.

The internet is often utilized to promote and support acts of terrorism by using the following activities:

Online terrorist-related Hate speech

Online terrorist-generated content

Online financing of terrorism

Online recruitment and training of terrorism

This is often not immediately. recognizable or obvious, so we provide some information and notes here to help y.ou recognize them better and protect and delimit y.ourself accordingly.

ONLINE TERRORIST-RELATED HATE SPEECH

What is online terrorist-related speech?

Any kind of online communication that promotes or justifies racism, xenophobia, anti-Semitism or other forms of intolerance based on hatred, including intolerance in the form of aggressive nationalism and ethnocentrism, discrimination and hostility towards minorities, migrants, and people with a migration background.[1]

Individuals and groups can be affected by hate speech by terrorist groups or their sympathizers. As a result, they experience:

Racism and Xenophobia (discrimination based on ancestry),

i.e. rumours about criminal offenses, incomplete information, subjectively filtered reporting towards other ethnic communities

Anti-Semitism and anti-Muslim racism (discrimination e.g. against Jews and Muslims)

i.e. there are whole topic blogs that are devoted to inciting hatred aimed at Muslims or defaming associations and mosque communities; stereotypes of an impending Islamization are often used here.

Important: If these are not contradicted (even by those who think differently), it can give the people concerned the feeling of being excluded, rejected and not respected because of their family origins or religious affiliation.

But what is typical for hate speech? How can you recognize this type of communication? [2]

Us vs. them rhetoric (referring to an ingroup / outgroup - e.g.: "They threaten “our" women. "Politicians support the Islamization in our country")

Deliberate dissemination of uninformed or false statements (e.g. statements such as: "The refugees do not have to pay in the supermarket.") ☞ [Fake news]

Disguise as humour or irony (e.g. sentences like: "I also want a new smartphone. In my next life I will become an asylum seeker.")

[1] for similar definition see: Council of Europe's Committee of Ministers: Recommendation No. R (97) 20 of the Committee of Ministers to Member States on 'hate speech

[2] „Hate Speech – Hass im Netz Infobroschüre" from Lsm, ajs & Kooperation with klicksafe.de (https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_Allgemein/Hate_Speech_lfm_ajs_klicksafe.pdf)

- **Degrading and denigrating terms**; **sexist and racist insults** (e.g. insults such as: “A woman shouldn’t be working somewhere like this”, “Go back to your own country”.)

- **Serving stereotypes and prejudices through certain terms and language patterns** (e.g. terms such as: "Asylum seekers.", "Foreigners out.", "Threatening Islamization.")

- **Generalizations** (statements like: "All gypsies are lazy.", “Immigrants are stealing our jobs”.)

- **Striking imagery** (racist depiction, e.g. of black people with bast skirts; images that reproduce stereotypes)

For more information, advice or reporting see: *www.stophateuk.org*

ONLINE TERRORIST-GENERATED CONTENT

The term **"terrorist-generated online content"** refers to the online dissemination of statements aimed at motivating other persons, directly or indirectly, to commit a terrorist crime, for example by glorifying the latter.[3]

Terrorists use the Internet for the **dissemination of propaganda**. Propaganda generally takes the form of multimedia communications providing explanations, justifications or promotion of terrorist activities, for example in, audio and video files and video games

Online propaganda includes contents such as video footage of violent acts or video games developed by terrorist organizations that simulate acts of terrorism. A broad range of tools are used, for example websites, virtual chat rooms and forums, online magazines, social media platforms, and popular video and file-sharing websites to disseminate propaganda. 4 Particularly social media platforms such as Twitter and Facebook, and popular video and file-sharing websites, such as YouTube are prominent tools for radical group to publish their propaganda **containing violence, hate and fake information**.

☞ [Safety & Social Media] [Fake News]

The promotion of violence is very common in terrorism-related propaganda and its distribution via the Internet greatly increases potential victims.[4] Furthermore, extremist groups disproportionately **target youth** (adolescence and young adults) to spread propaganda as they are more vulnerable to extremist ideas and dangerous behaviours.[5] [6]

☞ [Child protection on the Internet]

Propaganda encourage potential or actual sympathizers through messages conveying pride, accomplishment and dedication to an extremist goal. For example:

- Advocating or calling for acts of violence (e.g. "They should all be shot / burned / gassed.", "On the gallows with them!")
- The glorification of terrorist attacks with the aim of persuading other actors to imitate them (e.g. "9/11 was a great revenge on the infidels. Further punitive actions should follow.")
- Demonstration of the effective execution of terrorist attacks to those who might be ready to adopt such behaviour

[3] a comparable definition can be found in the EU - Regulation on combating terrorism, Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism

[4] United Nations Office on Drugs and Crime (2012). The use of the Internet for terrorist purposes. In collaboration with the United Nations Counter-Terrorism Implementation Task Force. Retrieved from: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

[5] Hassan, G., Brouillette-Alarie, S., Alava, S., Frau-Meigs, D., Lavoie, L., Fetiu, A., ... & Sieckelinck, S. (2018). Exposure to extremist online content could lead to violent radicalization: A systematic review of empirical evidence. International Journal of Developmental Science, 12, 71-88.

[6] Harpviken, A. N. (2019). Psychological vulnerabilities and extremism among wyestern outh: A literature review. Adolescent Research Review. doi:10.1007/s40894-019-00108-y

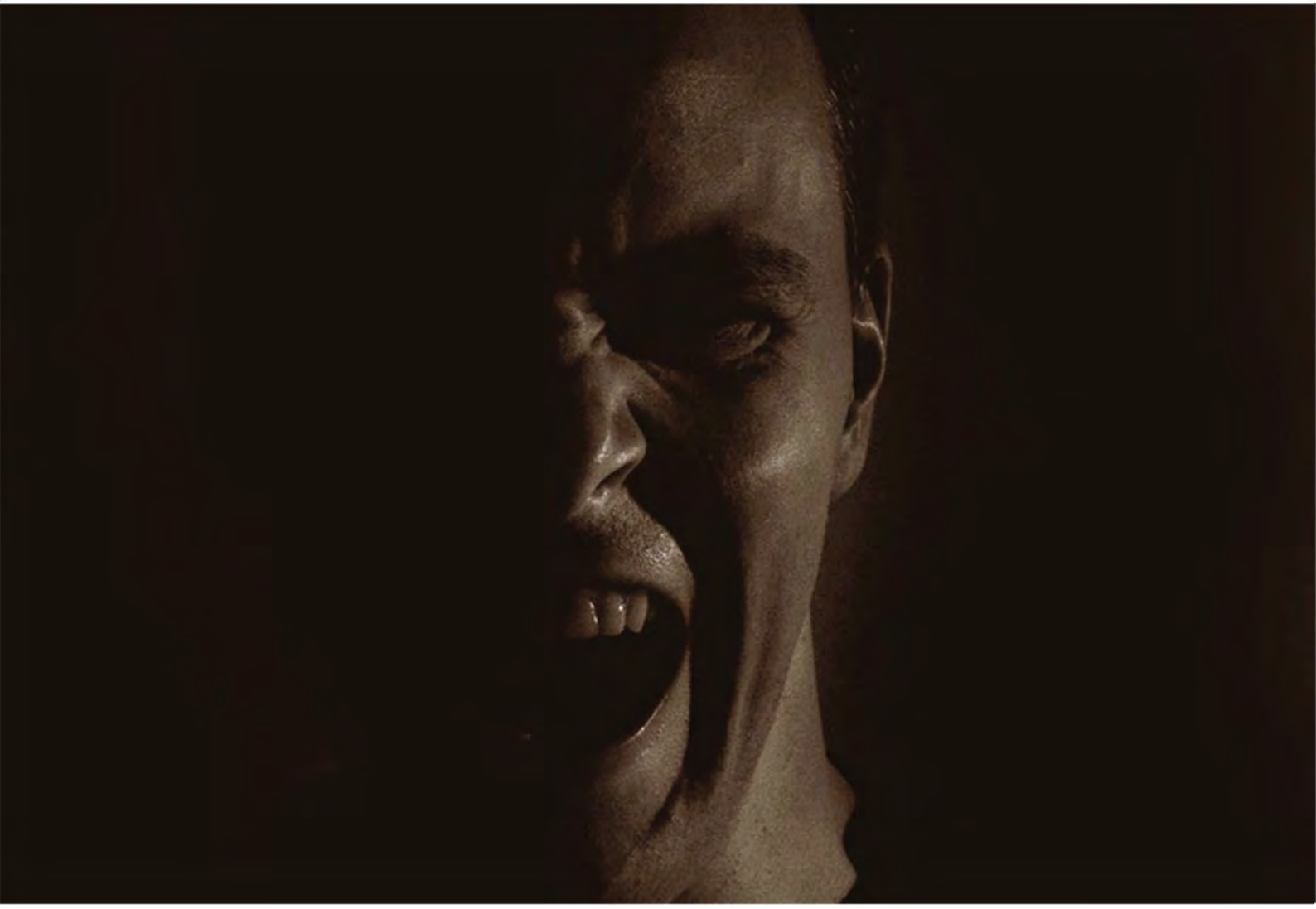
If you discover a page that contains false reports or content that is inhumane, you can report the page to the relevant operators (e.g. Facebook see https://www.facebook.com/help/263149623790594?rdrhc)

To report online material promoting terrorism and extremism please visit: https://www.gov.uk/report-terrorism

If you have ***a relative, friend or other person*** *you are concerned about, please see* ***[Advice hotline]***

Childline will help anyone under 19 in the UK with any issue they're going through.

If you want to talk about anything. Whether it's something big or small, the trained counsellors of Childline will support you. Call them for free on ***0800 1111*** *or see https://www.childline.org.uk/about/about-childline/*



ONLINE FINANCING OF TERRORISM

Online financing of terrorism comprises the provision or acquisition of financial resources on the Internet with the aim that these are used in whole or in part to carry out terrorist offenses, or at least in the knowledge that the corresponding funds are (should) used for this purpose.[7]

Terrorist organizations and supporters may also use the Internet to finance acts of terrorism. To raise and collect funds and resources for terroristic endeavors, four strategies are used:[8]

direct solicitation,
e-commerce,
the exploitation of online payment tools and
through charitable organizations

Direct solicitation refers to the use of websites, chat groups, mass mailings and targeted communications to request donations from supporters.

E-Commerce: Websites may also be used as online stores, offering books, audio and video recordings

Online payment facilities offered by websites or communications platforms make it easy to transfer funds electronically between parties. The transfer of funds is often made by electronic wire transfer, credit card or alternate payment facilities available via services such as PayPal or Skype. Additionally, fraudulent means such as identity theft, credit card theft, wire fraud and stock fraud may be used to fund terrorism.[8]

General advice on cybersecurity and tips for a safe internet experience see ☞ **[Cybersecurity]**

Charitable organizations: terrorist groups have been known to establish organizations that may claim to support humanitarian goals while in fact donations are used to fund acts of terrorism.[8]

Particularly on social media platforms, information provided by users may be misappropriated and used for the benefit of criminal activity. ☞ **[Safety and Social Media]**

[7] a comparable definition can be found in the EU anti-terrorism regulation Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism

[8] United Nations Office on Drugs and Crime (2012). The use of the Internet for terrorist purposes. In collaboration with the United Nations Counter-Terrorism Implementation Task Force. Retrieved from: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

ONLINE RECRUITMENT AND TRAINING OF TERRORISM

Online recruiting is the process of recruiting someone else on the Internet to commit terrorist offenses or to assist in their implementation. Online training refers to the training of other people or the participation in training courses on the Internet with the following content: Production or use of explosives, firearms or other weapons or toxic or dangerous substances or other specific methods and techniques with the aim of a terrorist committing a crime or participating in its implementation.[9]

The reach of the Internet provides terrorist organizations and supporters with a global pool of potential recruits. Internet platforms provide detailed instructions, often in easily accessible multimedia formats and multiple languages, on **topics such as how to construct explosives, firearms or other weapons or hazardous materials; and how to plan and execute terrorist attacks**. The platforms act as a virtual training camp. Restricted access cyberforums offer a platform for recruits to learn about andto engage in terrorist actions.[8]

Terrorist propaganda is often tailored to appeal to vulnerable groups in society and focus on sentiments of injustice, exclusion or humiliation as part of the process of recruitment and radicalization.

The Internet may be a particularly effective medium for the recruitment of minors, who comprise a high proportion of users. Tactics employed to target minors include mixing cartoons and children's stories with terrorist messages.[8]

☞ [Child protection on the Internet]

ADVICE HOTLINE

Anyone who is concerned about a relative, friend or other person they know becoming radicalised, can call the **Anti-Terrorism Hotline on 0800 789 321**.

They can also report it to their local police force, either via **101 or online**, where the reporting person may be asked to complete the **National Prevent Referral Form**.

For concerns about a child becoming radicalised, the **NSPCC** can also be contacted on **0808 800 5000**, or by email at ***help@nspcc.org.uk***.

[9] similar definition in Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism

SAFETY AND SOCIAL MEDIA

Particularly in the age of **Facebook, Twitter, YouTube, and similar platforms**, individuals publish sensitive information on the Internet. Whether voluntarily or inadvertently, some of this information may be misappropriated and used for the benefit of criminal activity.

Basic considerations:

Before you sign up for a social network, you should ask yourself: **"What expectations do I have from participating in this network?"**

- Should it be for private use, so that it is important that only your friends can find you?
- What do you want to achieve with your profile? Should it be a purely private profile for you or is it (also) intended for business use - hence also possible that you can be contacted by third parties?

For your data protection:

- It is very helpful to use a **separate e-mail address for each network** - this may be more of an effort at first, but it protects your privacy a lot more.
- Think carefully about whether you want to appear under your real name or under a **pseudonym** - what should be clear to the public?
- Should your profile content be accessible by everyone (public) or just people you know?
- To make it **difficult for strangers to access your data** (such as photos and profile content), resist the temptation to indiscriminately add every possible profile as a friend - you never know who is actually behind it.

Privacy settings on Facebook, Twitter and Co.:

- Many social media platforms offer the setting option *"Make profile invisible to search engines"* - this is sometimes hidden - but it can be very helpful if you don't want to be found on the first Google hit. If the setting option is not apparent, contact the network's help center if necessary.

- Activate the *"Privacy Checkup"* and verifying function e.g. Facebook - this means that all contributions and markings in which you appear must first be confirmed by you before they become visible to the public.

- You should *not make your contact details visible* to anyone unless you are using your account for business.

- Visibility of your content: Posts, profile pictures, photo albums ... in most networks you can choose exactly who can see which content. The following applies here: *the less publicly visible, the better.*

The difficulty with Personal Data

Many people still handle their personal data too lightly without being aware of how much it can be worth for individual companies or authorities, e.g. to better predict their activities and interests and accordingly personalized advertising and to be able to place and present offers.

Examples of **personal data recorded**:

° Location data
° Contact details
° Information about consumer behaviour.

In this way, tailor-made content for advertising can be created and displayed. This enables companies to generate millions of dollars in profits – **so personal data actually is worth cash.**
On the other hand, this *sensitive information, should it fall into the wrong hands, can cause great damage and be misused* - for example, criminals can tap bank data to access third-party accounts or to create/sell wrong documents with personal or ID numbers etc. ☞ **[Cybersecurity]**

So always be careful not to give away too much personal information, especially if it is not absolutely necessary!

Additionally, here you can find a short YouTube tutorial about why data protection and privacy is important:
https://www.youtube.com/watch?v=ZNEPaGFApX4

How can I ensure my data security?

Secure https encryption:

You should always make sure to choose a **secure data connection** when surfing (**identified by https //: - the "s" stands for "secure"**). This encrypts the data so that your online activities and the information you enter cannot be viewed or intercepted by third parties.

For detailed information see *https://www.youtube.com/watch?v=w0QbnxKRD0w*

Surfing incognito:

Here's how to enable incognito mode for private browsing in *Chrome, Microsoft Edge, Internet Explorer, Mozilla Firefox, Safari*, and Opera: *https://www.lifewire.com/browsing-incognito-445990*

There are very simple ways to provide more security that can be implemented without much effort. Cookies are also a big topic.

And what are Cookies?

On almost every website you are asked whether you agree to the use of cookies or not. They are text files that are sent by your browser to the relevant server on the site. In this way, the pages can call up and "remember" information from your previous visits.

Thus, the content can be tailored to the user and his typical surfing habits. **If you agree to the cookies, your personal data will be stored and, for example, evaluated by online shops**.This allows a fairly accurate motion profile to be created of the user.

However, accepting cookies can be useful on pages that are used regularly: To avoid having to login again or repeatedly having to fill forms.

A short explanation & how cookies work, you can find on this YouTube video: *https://www.youtube.com/watch?v=QWw7Wd2gUJk*

CHILD PROTECTION ON THE INTERNET

It is not always easy to have a complete overview of all the opportunities given by the Internet, especially for parents. Some parents may be worried or feel unprepared about how to protect their children against attacks by radical groups.

Here you will find some information on how to recognize extremist content on the Internet and how to sensitize your child to dealing critically with potentially radical online content – even if it initially seems inconspicuous.

Firstly, common ideas must be rethought, for example the idea that right-wing extremist groups only deal with **"typically right"** topics and contents. It is usually the other way around - they look for content and subject areas that are (often also for young people) widely concerned in society and which may be actively and intensively discussed. Often, opinions are presented here that are emotional and met with broad approval in society.

Radical groups often attempt to spread extreme opinions in disguise and make them *appear socially acceptable and normal.* It is not uncommon, that this way also misinformation is spread or historical events distorted. These are strategies to create ill feelings towards minorities. Additionally, pages of extremist groups are usually designed very professionally to make a serious impression.

> ***Therefore, it remains inevitable to accurately check posts or websites - if possible together with your child – to determine whether the source of information and the page is reliable and what source this information is based on.***

How can I protect myself and my child?

It is crucial to give your child support and enable them to tell apart:
• Which information is real?
• Which is not?

A basic building block is:
• To talk to your child about what is going on in the world already at an early age and
• To encourage them to develop a differentiated perspective on these events and information

The key element is to question information and to be able to classify and differentiate opinions and news. It should also be clearly stated that there are people who specifically disseminate misinformation (e.g. for the purpose of making money or influencing opinions). It is important to **remain critical** - even if information has already been shared often (e.g. via social media) or if a page appears serious at first glance - neither is evidence that the information presented must be true.

For more advice see; https://www.saferinternet.org.uk/
You can report any concern at: https://www.ceop.police.uk/safety-centre/

For further information please see
https://www.youtube.com/watch?v=yjAmB0UHnHE

FAKE NEWS

Nowadays, every online user can easily write their own posts and share their opinion via their own blogs, comments or in social media. At the same time, the newly gained diversity poses a greater challenge than before to online users having to decide for themselves which published information is right or wrong.

From chain letters via messenger or e-mail to social media posts with linked incorrect content: **many online users are confronted with dubious content on the Internet every day.**

Which sites help to educate about fake news and false reports?

- Fake news: What is it? And how to spot it: *https://www.bbc.co.uk/newsround/38906931*
- Independent UK fact checking site: *https://fullfact.org/*
- UK Government resources to enable fact checking of information: *https://sharechecklist.gov.uk/*

Dealing with fake news / inhuman content

If you discover a page that contains false reports or content that is inhumane, you can:

- report the page to the relevant operator
  (e.g. Facebook see *https://www.facebook.com/help/263149623790594?rdrhc*)
- or (e.g. if a crime is suspected) also send your concerns about the page to external complaints offices (with a corresponding screenshot)

Complaints offices are e.g.

- UK television or radio complaints - *www.ofcom.org.uk*
- UK Advertising standards agency - *www.asa.org.uk*
- Newspapers or magazines who are members of the UK Independent Press Standards Organisation - *www.ipso.co.uk/complain*

Evaluating online sources[10]

How do you determine if a source is credible? You can evaluate the reliability and scholarship of information you find both online and in print by using these guidelines:

- **Authorship**

If the author is not identified be wary. When an article or website is authored anonymously it has little credibility. It should be evident who created the content. What are the author's credentials? Does he/she have expertise in this field? Is biographical information provided?

- **Publisher**

This can help you determine the origin of the document, for example whether it is produced by an established publisher, a government agency, a nonprofit organization, or a commercial website. Consider the publisher's reputation and trustworthiness.

- **Accuracy and objectivity**

Can the facts presented on a website be substantiated elsewhere? Beware of information that can't be confirmed or that presents a biased view. Always check multiple sources to determine credibility.

- **Timeliness**

Be aware of when the web page was created and how recently it's been updated. Is the information current? Outdated information and broken links indicate the page is not being maintained.

- **Footnotes and bibliographies**

Legitimate references and links to other sources can add to a document's credibility and depth of scholarship.

- **Sponsorship**

Some sites are officially approved by the parent organization to which they're linked. Others can be on a parent site but not officially sponsored by the organization. A personal homepage on a university's server does not automatically confer credibility.

[10] https://library.columbia.edu/libraries/undergraduate/evaluating_web.html

CYBERSECURITY

It may not always be easy for you to identify all the dangers lurking for you on the Internet and what you can do to counter them. In the following text, we have summarized a few important tips and tricks ready for you, so that you can move around the Internet more safely and with a keen eye.

A brief overview about the most important information about secure passwords:

A secure password should:

- be at least **eight characters long (more if possible)**
- contain **Lower-Case and Capital letters, numbers and special characters**

! Avoid !

- only combination of Dictionary Words (e.g. red house)
- logical series of numbers or letters (e.g. birth dates)

Instead, create passwords that:

- Try to mix it up so it fits many of the requirements —for example, “BigHouse$123”
- reflect a **personal sentence** —for example, “The first house I ever lived in was 613 Fake Street.” So your password would become Tfhleliw613FS.
- based on completely **unreflected** series of characters (e.g. hdg6tzfrsgj5n6jlGHG).

And use if possible

- a new, secure password for each registration.

Because if one of those passwords is cracked (no password is 100% secure!), at least the other accesses remain protected.

Here you can find a short YouTube tutorial that explains the creation and importance of passwords: *https://www.youtube.com/watch?v=aEmF3IyIvr4*

In addition to a secure password, the following security measures are as important:

Virus protection
Firewall
careful handling of login data

Consortium

Hochschule für den öffentlichen Dienst in Bayern
Fachbereich Polizei

CENTRIC
Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research

POLICE SERVICE NORTHERN IRELAND

POLICEJSKA AKADEMIJA MUP RH

AGENFOR INTERNATIONAL

iti CENTRE FOR RESEARCH & TECHNOLOGY - HELLAS
Information Technologies Institute

Ministero della Giustizia

Freie Universität Berlin

europeaninstitute

Politsei- ja Piirivalveamet

UNIVERSIDAD DE GRANADA

RSM Erasmus

KEMEA

Politie
Voorkempen

Coordinator PROPHETS

Dr. Holger Nitsch

University of Applied Sciences for Public Service in Bavaria — Department of Policing

Fürstenfelder Str. 29
82256 Fürstenfeldbruck
Germany

Prophets Project

www.prophets-h2020.eu

@H2020Prophets

Project-Prophets