



VALG

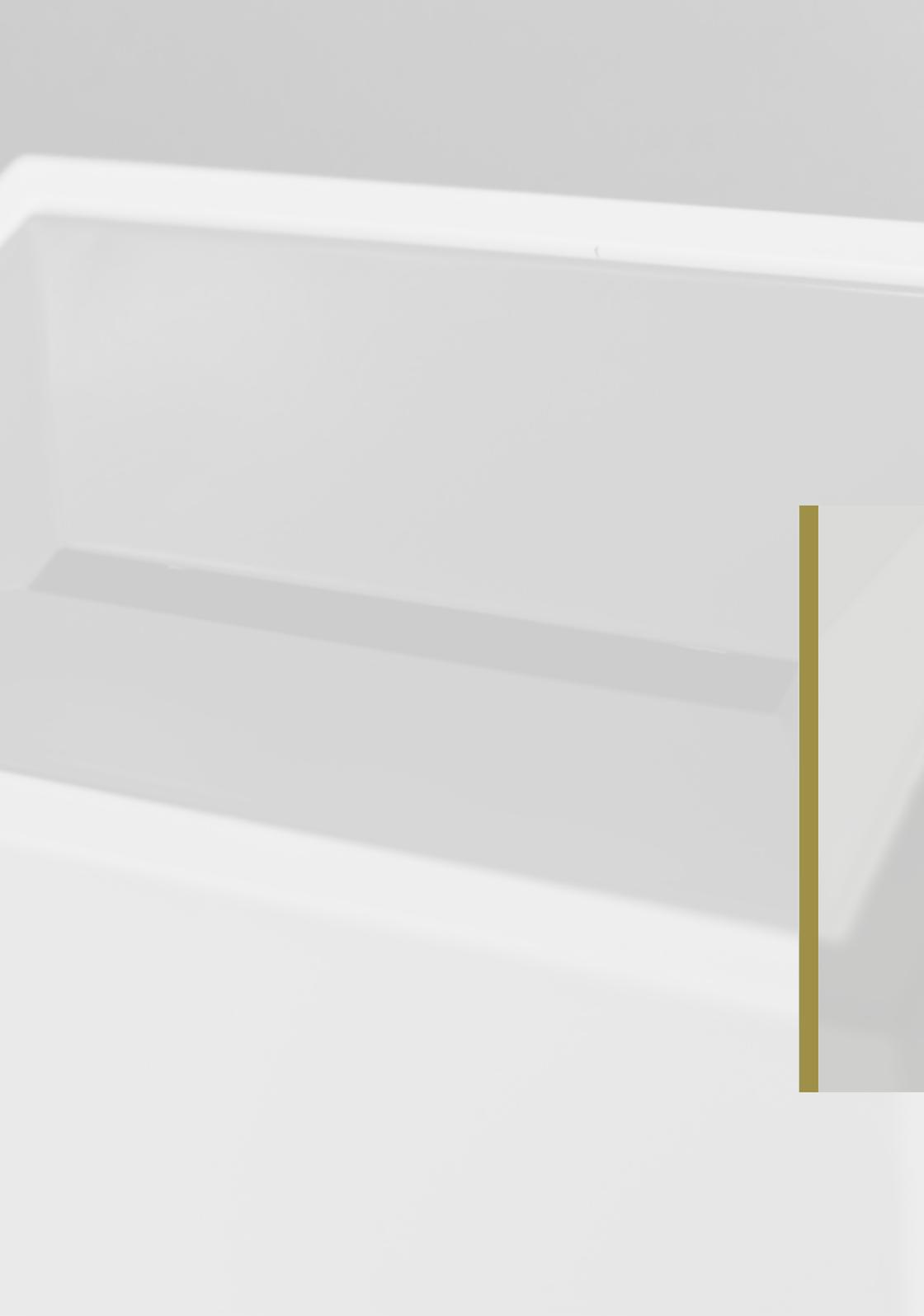
English

You are of interest –

Useful advice for you as a political candidate

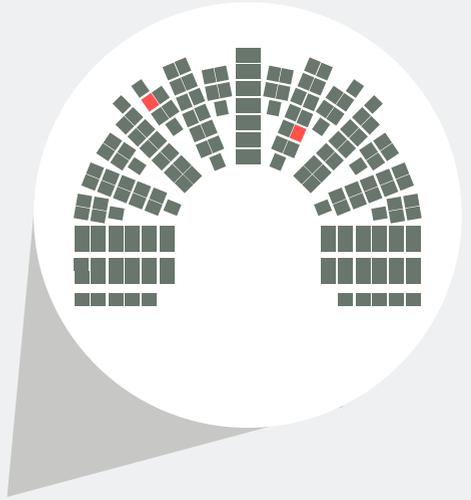


Prepared by the Norwegian
Intelligence Service, the
Norwegian National
Security Authority and
the Norwegian Police
Security Service



Contents

Norway – a society based on trust	5
Your information – your responsibility	5
You are of interest	5
Know your values	8
When should you ask for advice?	10



Norway – a society based on trust

The last year has seen an increased awareness about the danger of foreign states attempting to influence political processes in other countries. In this context, influence can be defined as a foreign, government-initiated, covert and deliberate activity carried out to achieve either a short-term or long-term goal that could weaken Norwegian interests, for the benefit of another state. These attempts to influence can be aimed at the electoral system and how the election is conducted, or at political actors, voters and attitudes held by the population.

We have a well-functioning and stable democratic system and a society characterised by openness. This contributes to a certain level of resilience within our institutions and among individuals who hold political positions. Norway thus has a solid foundation to resist such attempts to influence our domestic political processes. But we mustn't be naive.

Foreign states will still be able to seek out information about Norwegian politicians, political processes or attitudes and influence them. Each and everyone of us can help to safeguard sensitive information about ourselves and our political processes, and deal with any potential attempts to influence them.

Your information – your responsibility

You can personally contribute by protecting your information and the tools you used to communicate. The actions you take have an impact on your own integrity and your ability to communicate safely and securely. It is important that you understand how to deal with situations that may pose a risk. These could include times at which you must interact with other people or use digital tools.

You are of interest

Foreign states' intelligence services conduct targeted operations in Norway. These operations are particularly aimed at those who have conflicting or competing interests. As a politician, this means that you will have to consider the fact that, as part of their activities, foreign states' intelligence services may be interested in you. They use both overt and covert methods to achieve their objectives. Detailed information about you, either as a private individual or as a politician, could prove to be particularly valuable. These

intelligence services are highly skilled at creating relationships between people, namely through pleasant and natural meetings. Even something as seemingly mundane as your phone's contact list could be of interest to these services. This relationship could be exploited negatively later on.



FAKE EMAILS

Emails are constantly being sent out claiming to come from well-known companies, for example emails from the company supposedly sending an invoice. In some cases, clicking on a link in the email or opening any of the attachments may result in malware being installed on your computer, while in other cases, the sender may be looking to obtain information about you, such as your login details and other data that could be used at a later date.



HUMAN APPROACH

A Norwegian politician may come into contact with a diplomat, delegation member or business owner. The politician is later invited to lunch. This lunch is followed up by several other meetings held over a longer period. The politician is asked for information about others in the party, or a rival party. This may be work-related or of a personal nature. The person also asks the politician to set up meetings with the leader of the party or with other parties of interest. Foreign actors, as mentioned in the example, may be affiliated with or could be being exploited by the country's intelligence services. This is a common way of operating in Norway.



Exploiting vulnerabilities

Foreign states are constantly working to break into computer systems to extract information, or to take over the systems entirely. Insiders are central to the success of such activities. These are people who already have legitimate access to both the information and the systems. Tricking people into allowing them access happens on a daily basis.

The simplest method of hacking into computer systems is to get recipients of emails to open attachments or links that then initiate the technological attack. Information, for example that of a sensitive and private nature or about political attitudes, can be exploited.



Know your values



Know what qualifies as sensitive information for you and your party

- ▶ What information holds the greatest value and the most serious consequences if others gain access to it?
- ▶ Who can you share such information with and who must it not be shared with?



Handle sensitive information with caution

- ▶ Think about what you say and who could be listening – both over the phone and when in public.
- ▶ Make sure you have confirmed the identity of the person you are communicating with.
- ▶ Certain topics or cases should not be discussed over the phone or sent via your regular email or text.
- ▶ When something is deemed as sensitive, meetings about it must be conducted without the presence of PCs, phones or smartwatches.
- ▶ Use encryption solutions for your electronic communication.



Protect your mobile phone, tablet and PC

- ▶ Do not loan your electronic equipment to others.
- ▶ Keep your electronic equipment updated with the latest versions of any software you are using.
- ▶ Do not allow others access to your PC, mobile phone, USB flash drive or other electronic equipment.



Protect your digital services

- ▶ Use multi-factor authentication (use of passwords in combination with text, security code generators or similar) where the option is available.
- ▶ Use different passwords for different services.



Email

- ▶ Be critical of any links and attachments in emails you receive.
- ▶ If you are unsure whether you should open an attachment or link – first assess whether it is absolutely necessary.
- ▶ Get in touch with the sender via phone/another way if you're still unsure.
- ▶ You could also do an internet search for the information without opening the link/attachment.
- ▶ Report suspicious emails to your party organisation, trade union representative for your list or employer.



Social media

- ▶ Use the available privacy settings to protect access and visibility to these as required.
- ▶ Be aware of what you post about yourself and others.
- ▶ Be critical of anything that may be fake news – avoid sharing further.
- ▶ Turn off options to share your location if you absolutely do not need to do so.
- ▶ You must also inform others that you do not want them to tag you and your location on social media
- ▶ Apply to have your Twitter account verified and do the same for other similar services when the option is available. Doing so significantly increases the credibility of your account. Remember to use a strong password.



Travelling

- ▶ Avoid using public WiFi. Use your mobile data or mobile broadband instead.
- ▶ If you are travelling to a vulnerable country, you should not take your regular mobile phone, PC or tablet. Vulnerable countries include those that Norway does not cooperate with regarding security policy.

When should you ask for advice?

Get in touch with your party organisation, trade union representative or employer if you:

- ▶ Receive any suspicious emails
- ▶ Experience technical irregularities in your digital equipment
- ▶ Lose your mobile telephone, PC or tablet
- ▶ Lose any sensitive information
- ▶ Are on the receiving end of a targeted approach
- ▶ Find that your social media profiles are being misused
- ▶ Are involved in the sharing of false information

If you think you have been the victim of a digital attack, or are being influenced or targeted by foreign states, you should inform your immediate manager to discuss the matter as soon as possible. What should you do if you're still concerned?

Contact the relevant authorities, such as the Norwegian Police Security Service (PST), the Norwegian National Security Authority (NSM) or the local police.



SUSPICIOUS EMAILS

- ▶ Check if the sender is authentic. E.g. If the email: contains any incorrect letters, ends in .com instead of .no; or is registered as a Gmail or Yahoo account rather than a work account
- ▶ If you recognise the sender, but are still unsure – call them to check whether they have actually sent you something
- ▶ If it's too good to be true, then it probably is – use common sense!





*This brochure has been prepared by the
Norwegian Intelligence Service, the
Norwegian National Security Authority and
the Norwegian Police Security Service on
behalf of the Norwegian Ministry of Defence
and the Norwegian Ministry of Justice and
Public Security, coordinated and funded by the
Norwegian Ministry of Local Government and
Modernisation*