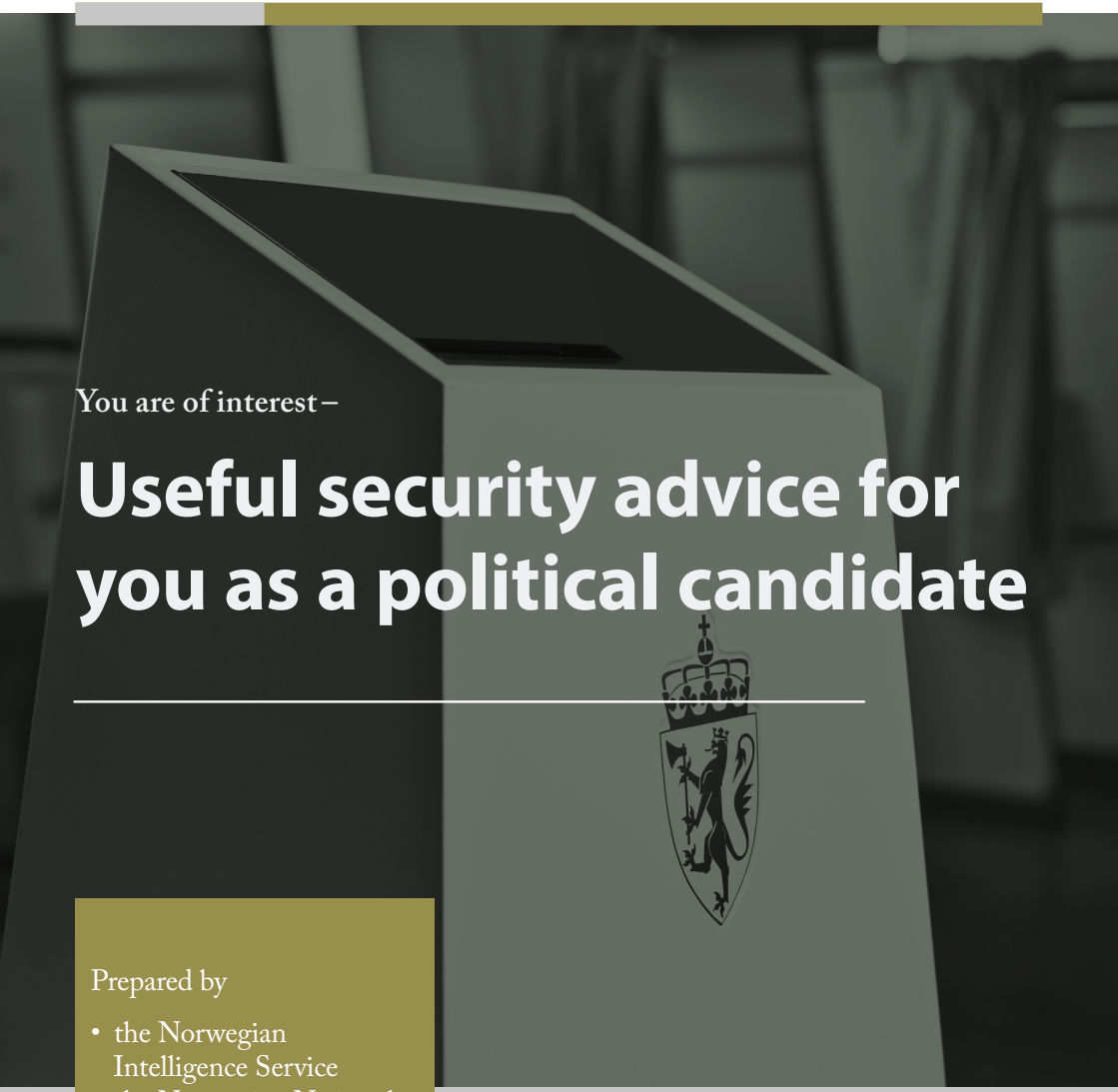
VALG

English

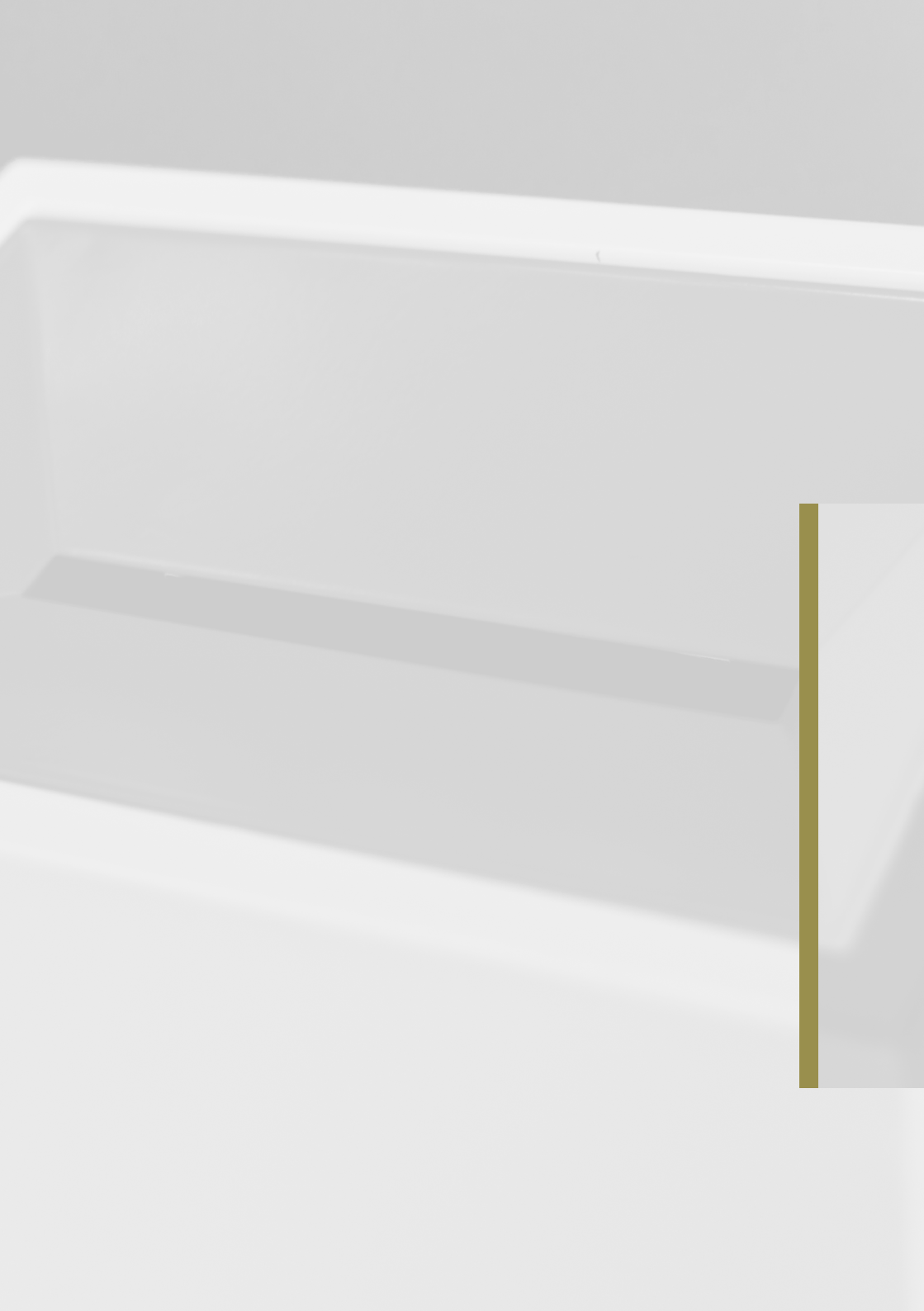


You are of interest –

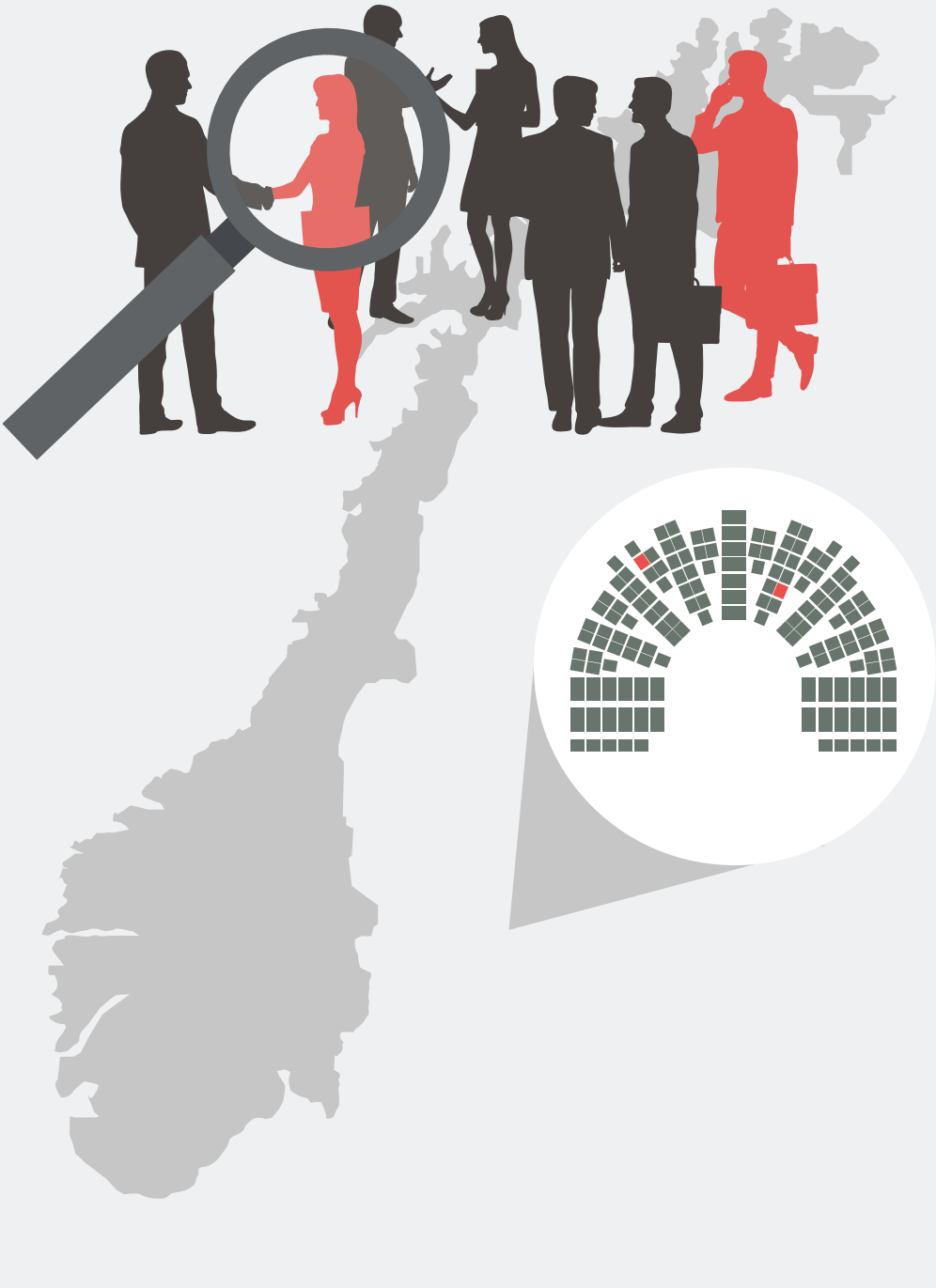
Useful security advice for you as a political candidate

Prepared by

- the Norwegian Intelligence Service
- the Norwegian National Security Authority
- the Norwegian Police Security Service



Contents



Norway – a society based on trust

The last year has seen an increased awareness about the possibility of both foreign states and non-governmental actors 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 how the election is conducted, at political actors or at 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 security 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 candidate for elections, 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.

FAKE EMAILS

Emails are frequently being sent posing as something they are not. The senders rely on trust, fear or temptations. For instance, someone may impersonate your bank and request that you sign in to solve a problem. Once you click on a link or open an attachment, the risk increases that your device is taken over by others, or that they are able to obtain your sign-in information or other important information that can be further exploited.

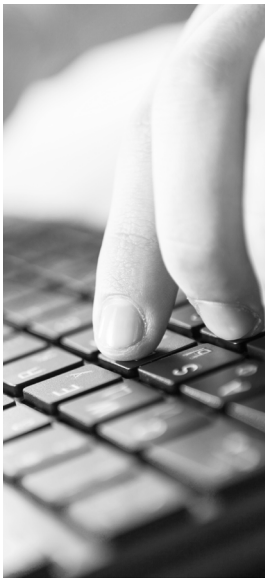
HUMAN APPROACH

A Norwegian local politician may come into contact with a 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 and other actors 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 or have had legitimate access to both the information and the systems, and who misuse this knowledge and access in a way that inflicts harm or losses to others. 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.



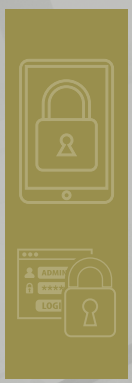
Know your values

Know what qualifies as valuable 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?

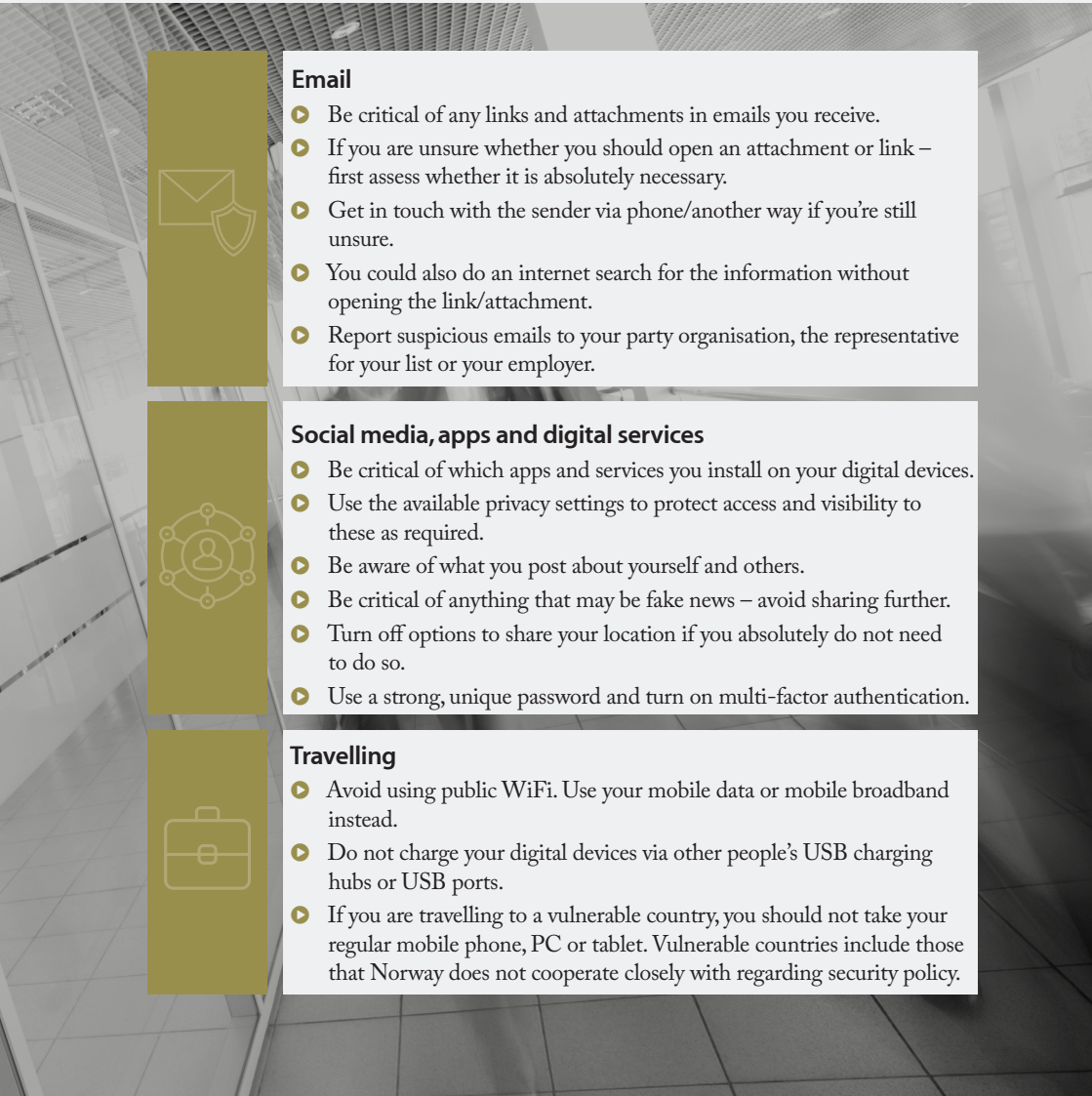
Handle sensitive information with caution

- Think about what you write/say and who could be reading/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 digital equipment and your digital services

- Do not loan your digital devices to others.
- Activate screen lock and preferably use fingerprint or facial recognition to avoid others viewing your PIN code when you unlock the device.
- Keep your electronic devices updated with the latest versions of any apps or software you are using.
- 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, the representative for your list or your employer.

Social media, apps and digital services

- Be critical of which apps and services you install on your digital devices.
- 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.
- Use a strong, unique password and turn on multi-factor authentication.

Travelling

- Avoid using public WiFi. Use your mobile data or mobile broadband instead.
- Do not charge your digital devices via other people's USB charging hubs or USB ports.
- 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 closely with regarding security policy.

When should you ask for advice?

Get in touch with your party organisation, the representative of your list or your employer if you:

- receive any suspicious emails
- experience technical irregularities in your digital equipment
- lose your digital equipment, such as 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
- experience incidents such as the dissemination of false information

If you think you have been the victim of a digital attack, or are being influenced or experiencing unwanted approaches, you should inform your line manager to discuss the matter as soon as possible.

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

For more information about digital security, visit nettvett.no.

For more information about critical media literacy, visit medietilsynet.no.

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 Regional Development.