Nederlandse Emissieautoriteit
Dutch Emissions Authority

August 2020

Security measures for NEa registry users

This information leaflet is intended for users of the registries managed by the Dutch Emissions Authority (NEa). The NEa makes every effort to secure the registries against undesirable use. As a user, you also play a key part in the security of the registries. This information leaflet tells you all about the measures that you can take to use the registries securely.

The NEa manages two registries:

- the EU Emissions Trading Registry (CO_2 registry) in cooperation with the European Commission;
- the Energy for Transport Registry (REV) for trade in renewable energy units (HBEs).

You can find further details of the emissions trading system, energy for transport and registries on www.emissieautoriteit.nl.

Background

In the past, malicious persons identified marketable units as targets of fraud and theft. Together with national and international partners, the NEa works to prevent criminals from succeeding. This information leaflet will provide you with the tools to ensure that malicious persons cannot access your account in the CO_2 registry or REV using your computer.

Universal measures

Please observe the measures below when using a registry. You can take these measures without great effort or investment required.

General measures

- If you receive emails addressed by the NEa, verify that the NEa is the actual sender. You can read how to do so in the section on *'Communication verification'* later in this information leaflet.
- If you notice anything suspicious when communicating with the NEa (via email, telephone, documents or other means) or using a registry, please get in touch with the NEa Helpdesk immediately. The contact details of the Helpdesk can be found at the back of this information leaflet.
- Do not use programs that share files online (such as BitTorrent). Malicious persons may access your computer system through these programs.
- Only use secure USB flash drives on the computer via which you are logging into a registry. Unsecured drives may infect your computer system with viruses.
- Frequently inspect your account's transaction history for suspicious transactions.

Measures for your mobile phone

- Be careful in sharing your mobile number with others, as it weakens the security of the registries.
- Never log into a registry from your mobile phone, as you are running the risk of revealing your data to malicious persons. These data include your username and password as well as the SMS code that you receive on your phone.

- Configure a password or PIN to lock your mobile phone.
- If your phone is lost, have your provider block your SIM card immediately.
- When using a smartphone, make sure that the operating system is up to date in order to improve security.
- Only connect to secure Wi-Fi networks and never connect to public Wi-Fi networks.

  You can read more about secure smartphone use on https://veiliginternetten.nl/themes/mobiel/basisbeveiliging-mobiel/.

Measures before logging in

- Read up on the security risks of using the computer, Internet as well as email and learn the tips for secure computer use. For example, you can visit www.veiliginternetten.nl to do so. Optimise your computer's security and use it as securely as possible.
- Make sure that the computer system with which you want to log into a registry:
  - always has the most recent updates of the operating system installed;
  - has installed a virus scanner that is always updated with the latest virus definitions and which scans the system for viruses at least once a week;
  - does not have illegal software installed.
- If you use a Wi-Fi network, ensure that it is properly secured. Public Wi-Fi networks are not secure: https://veiliginternetten.nl/themes/draadloos-internet/openbare-wifi-netwerken/.
- Protect access to your computer using a password.
- Create strong passwords to access your computer and the registries. See the section on *What is a strong password?* If you cannot remember the passwords, store them in a reputable password manager. Do not ever keep them in the same location as your usernames or save them in an unsecured file on your computer.
- Never share your username, password and SMS code with others, not even with colleagues. The NEa will never ask for your password or SMS code.

Measures during login and use

- Preferably use the Firefox or Chrome browser. The REV does not function optimally in Internet Explorer.
- Always log in using the link to a registry as communicated by the NEa. Never click another link to a registry due to the risk of being presented with a fake website where you enter your login details.
- Do not allow others to watch when typing in your username and password.
- Always log off before leaving your computer. Lock your system (using the combination of Windows key + L on a Windows system), so others cannot access it while you are away.
- Never let your browser store your username and password.

Communication verification

The NEa, as well as the European Commission in the case of the CO_2 registry, have taken a number of measures for you to test the reliability of the information that you read and the messages that you get.

Websites

To make sure that you are working securely in the correct registry and that you are receiving the right information, we recommend that you take two steps when visiting our websites.

1. Verify the Internet address (URL) of the websites. This URL has to start as follows.
   - NEa website: https://www.emissieautoriteit.nl;
   - EU Login website for logging into registry: https://webgate.ec.europa.eu/cas/;
   - CO_2 registry website: https://unionregistry.ec.europa.eu/euregistry/NL/index.xhtml;
   - REV website: https://rev.emissieautoriteit.nl/.

2. Verify the validity of the certificate on the websites mentioned above. A valid certificate guarantees that your connection to the website is secure. To verify this fact, look for a closed padlock visible to the left of the URL. The exact representation differs between browsers and is found on the following websites.
   - Firefox: https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure; Chrome: https://support.google.com/chrome/answer/95617?hl=en;
   - Internet Explorer: http://windows.microsoft.com/nl-nl/windows/know-online-transaction-secure#1TC=windows-7;
   - Safari: https://support.apple.com/nl-nl/guide/safari/avoid-fraud-by-using-encrypted-websites-sfri40697/mac;
   - Opera: https://help.opera.com/en/latest/security-and-privacy/.

Do you see a broken lock, an exclamation mark, a red or black cross, or any other warning signal rather than a closed lock? If so, please do not continue logging in and get in touch with the NEa Helpdesk.

Email
The NEa always includes a digital signature in the messages that it sends about the registries and their security:
- Click the certificate sign in the email.
- Click 'Details'.
- Click 'View details'.
- Click 'Show certificate'.
- The 'Certification path' tells you that the certificate hails from QuoVadis Issuing CA G3.

Please note: some certificates are sent as an attachment. This situation is often the case if you read messages through Webmail. If so, you will not be able to follow these verification stages.

Further measures
If your computer is part of a large corporate network, its security is the responsibility of the network's ICT managers. Apart from taking the measures described above, there is little that you can do yourself to improve the security of your computer. You can have the ICT managers read this information leaflet, however, and have them assure you that the network environment is secure. The measures below could be considered if you are working on a separate computer or using a network that you manage yourself.
- To access a registry, consider the use of a special computer that does not perform any operations other than accessing the registry and that is not connected to other computers (e.g. through a network). This measure greatly reduces the risks of your computer becoming infected with malicious software.
- Consider installing a program such as IBM Security Trusteer Rapport (free of charge) in addition to your normal virus scanner. Such programs are specially built to detect viruses and other malware aimed at retrieving login details or taking over your computer. They are a lot better than normal virus scanners at detecting these processes.

What is a strong password?
You will need a password to log into the registries. To this end, we recommend that you do not use a password that can easily be discovered by third parties. A strong password for the registry must meet the following requirements:

- It is at least eight characters long.
- It is not an existing word or a word that is easy to guess, such as your cat's or partner's name.
- It consists of:
    - capitals;
    - lower-case letters;
    - numbers;
    - symbols.

Never use the same password for more than one application. See https://veiliginternetten.nl/themes/situatie/mijn-wachtwoord-sterk-genoeg/ for the steps to create a strong password.

NEa Helpdesk
Have you noticed anything suspicious? Please contact the NEa Helpdesk as soon as possible by phone on +31 (0)70 4568050 or by email at *info@emissieautoriteit.nl*.

Disclaimer
No rights can be derived from the text above, nor is the NEa liable for any malicious activities on your account.