Computer Emergency Response Team (KZ-CERT)
"State Technical Service" of the National Security Committee Republic of Kazakhstan
Republic of Kazakhstan, Z05T3C6, Nur-Sultan, Mangilik Yel st., 55B
Office: 8 (7172) 55-99-97
Email: info@kz-cert.kz

KZ-CERT Recommendations for Safe Remote Networking

1. Comply with all security policies adopted in corporative infrastructure.
2. Store confidential information on removable media.
3. Do not share your workstation access to the third party.
4. Update router and, if necessary, password to access settings, furthermore, restrict the number of connected devices.
5. Update licensed software, you should also avoid third party internet resources.
6. Use strong password and, if possible, set up two-factor authentication.
7. Back up your data and store it separately from your PC to avoid negative consequences of intruders.

For Email Security Recommendations

8. Check links. Do not follow the links, even if they seem legitimate. You can always find additional information on your own.
9. E-mail attachments. Never open suspicious app! If you did not expect a letter or app, just do not open it.
10. Check e-mail addresses. Be sure about the sender's full mailing address and its legitimacy.

Computer Emergency Response Team (KZ-CERT)
"State Technical Service" of the National Security Committee Republic of Kazakhstan
Republic of Kazakhstan, Z05T3C6, Nur-Sultan, Mangilik Yel st., 55B
Office: 8 (7172) 55-99-97
Email: info@kz-cert.kz

KZ-CERT Recommendations for Safe Online Shopping

Due to high risk of customer data leakage towards e-commerce, KZ-CERT computer emergency response team recommends:

1. Always choose proven online shop only.
2. Scrutinize product or service feedback.
3. Purchase through official online shopping applications.
4. Verify the existence of the security certificate.
5. Use separate and virtual card for online shopping as far as possible.
6. Create a separate mailbox for registration in personal offices.
7. Do not make purchase via public WI-FI or use data. encryption when you purchase via public network.
8. Do not transfer prepayment or payment to unknown person.

Computer Emergency Response Team (KZ-CERT)
"State Technical Service" of the National Security Committee Republic of Kazakhstan
Republic of Kazakhstan, Z05T3C6, Nur-Sultan, Mangilik Yel st., 55B
Office: 8 (7172) 55-99-97
Email: info@kz-cert.kz

KZ-CERT Cyber Hygiene Basic Rules

1. Install licensed software. Update software products timely.
2. Check the PC regularly for malicious software.
3. Do not download and do not open suspicious files, as well as do not follow links of unverified sources.
4. Check your accounting data regularly and set strong passwords.
5. Be wary of the pop-up windows, the reports on your browser, operation system and mobile devices.
6. Use two-factor authentication.
7. Do not trust WI-FI access in public and do not enter your authentication data through open wireless networks.
8. Back up data regularly.
9. Do not comply with demands of extortionists and cryptographers.
10. Do not send copies of your documents containing personal data, identity documents, bank card details, etc.