K&H Bank Zrt.

1095 Budapest, Lechner Ödön fasor 9.
phone: (06 1) 328 9000
fax: (06 1) 328 9696
Budapest 1851
www.kh.hu • bank@kh.hu

Guidelines for the safe usage of K&H e-bank

E-bank, K&H Bank's netbank service allows you to do your banking in a fast and convenient way, from anywhere, 24 hours a day.

We are doing our utmost to ensure maximum security for this service. However, we also need some caution and co-operation on your part.

It is important to understand that the Bank does not monitor or supervise the operation of the Internet, and it bears no responsibility whatsoever for its safety. Internet fraud is a crime to be investigated by the Police.

1. What does K&H do to ensure the safety of e-bank services?

In providing e-bank services, K&H Bank applies security standards and procedures that ensure that the confidentiality of your personal and financial details is not violated, and such details are not disclosed to unauthorised third parties.

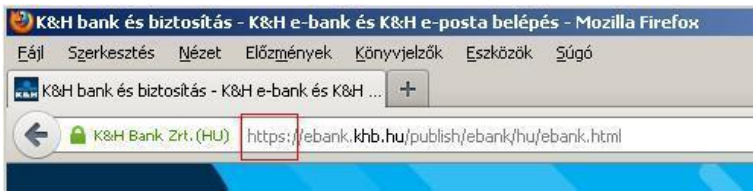
Secure connection

When you visit K&H Bank's website, a safe and encrypted connection is automatically established between your Internet browser and the Bank. Each piece of information you send or receive goes around the world wide web in an encrypted format, which unauthorised third parties are unable to read or modify.

One condition to establishing a secure connection is the checking of the e-bank server's 'identity'. Once a connection is established it also confirms that your browser indeed communicates with K&H Bank and not the system of a malicious attacker who may have diverted the connection.

Encrypted data transmission and the checking of the bank server's 'identity' are based on a digital certificate which can be regarded as the bank server's identity card. When, at the beginning of establishing the connection, the browser turns to the Bank's system, the server sends its certificate to the browser. If the browser finds the certificate to be in order, a safe connection is established. Otherwise, it warns the user of the problem.

The establishment of a safe connection is easy to recognise.



- In the address line, the bank's Internet address starts with 'https' (e.g. https://ebank.kh.hu)

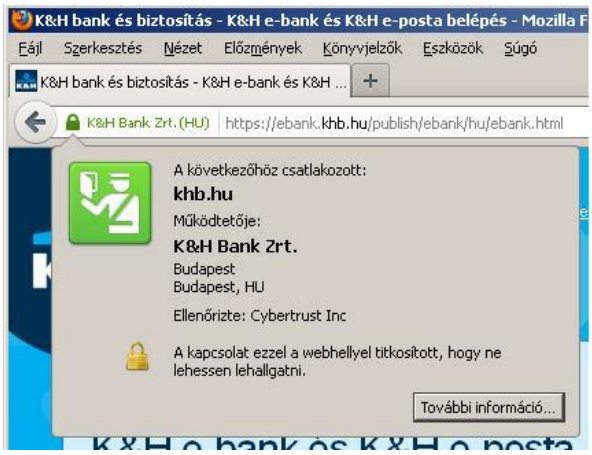
Internet Explorer

Firefox

- The browser displays a 'closed lock' symbol. The position of the lock icon depends on the browser's type and version number, but it is typically close to the address line, usually in front of it or behind.

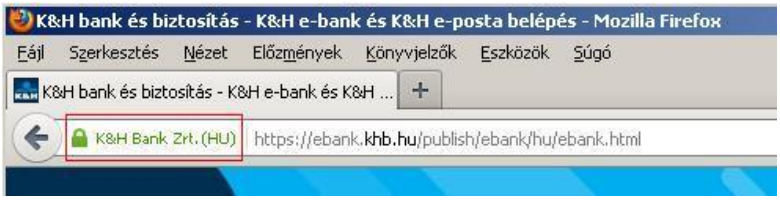
Checking of the digital certificate

Internet Explorer



Firefox

- The easiest way to check the certificate is by clicking on the lock symbol. By doing so you will normally receive a short summary about the certificate's contents. You can access more detailed information (the certificate's expiry date etc.) by clicking on the button/link under the summary.



- K&H Bank provides its public servers with so-called *extended validity* certificates, which offer even higher security than traditional digital certificates. In case of certificates of this type, newer browser versions display the owner's name in front of the address line (and the lock icon) in green, contrary to traditional certificates where the same are displayed in blue.

Secure identification of clients and transaction approval

E-bank, K&H's Internet bank **may be accessed in three different ways;** by way of chip card or SMS identification from traditional computers/laptops, or through a mobile application from smartphones (K&H mobile bank).

a.) E-bank with chip card identification

In order to ensure the safety of K&H's e-bank services, we use public key infrastructure (PKI), which allows us to apply digital signature to approve the log-in and the transactions. Cryptographic keys unique to users and required for the signature are stored on the chip card, under safe conditions.

The essence of the solution is that in this instance users also hold digital certificates, similarly to the server; i.e. both parties identify themselves to the other party using their 'digital ID cards'. The user's digital certificate can also be found on the chip card.

This solution ensures the meeting of the following requirements:

- **Confidentiality:** Messages may only be read by the Bank and the client, but not by unauthorised third parties.
- **Credibility:** The identification and checking of parties exchanging messages takes place subject to strong verification. The client verifies his/her transaction messages with his/her digital signature, and holds a digital signature certificate that allows this to be checked.
- **Integrity:** The digital signature defends the integrity (timeliness, authenticity and completeness) of transaction messages.
- **Undeniability:** Ensured by the parallel application of the digital signature and a time stamp.

What to do:

- Insert the chip card into the reader,
- Verify/sign transactions using the PIN code linked to the chip card.

b.) E-bank identified through text (sms) message

K&H Bank provides you access to its e-bank services not only subject to chip card identification, but also through log-in using a number sent by text (sms) message. In such instances, next to knowing the user name and password, you will also need access to the phone registered for the purpose of this service, in order to be able to log on and use the services.

In case of text message (sms) identification K&H Bank applies a daily transfer limit, the value of which is always set in the current Announcement.

c.) K&H mobile bank application

With the K&H mobile bank application, a reduced e-bank functionality becomes available following the identification of the user name and password. From a safety point of view, the following limitations must be expected:

- Funds may only be transferred to pre-entered (previously approved with a code sent in a text (sms) message or a chip card-initiated digital signature, in the traditional service fashion) accounts only.

- The maximum amount that can be transferred on a given day is limited.
- Certain functions available as part of traditional e-banking services are not accessible.

Automatic disconnection

If you log on to the e-bank service, but do not use it for a certain period of time, the Bank will automatically disconnect you. If you wish to continue using the e-bank service, you will have to log on again. This process helps make sure that others cannot access your details even if you forget to log off.

The monitoring of suspicious transactions

The bank monitors the transactions performed in the course of using the services, and if it comes across any suspicious events, it gets in touch with the client to clarify whether the transaction in question was indeed performed in line with the wishes of the authorised user.

2. What you need to do to keep your banking safe

The safe usage of K&H e-bank is also your responsibility, as we are not present in your home, and we do not monitor your computer or mobile device. If the device you use for getting access to the e-banking service gets infected; i.e. a virus or another malicious program gets installed onto it, it may threaten the safety of banking transactions.

Defending e-bank; in other words, defending your finances is similar to defending your home. Would you depart from your home and leave the door wide open behind you?

Make your computer safe

- If possible, use the service from a device that's under your control. Do not log on to e-bank e.g. from an Internet café or a public machine shared with others.
- Make sure you regularly install security updates issued for the operating system, the Internet browser or other software. If possible, use the automatic update function. This can prevent a situation where, exploiting known security weaknesses in the system, viruses or other malicious programs infect your device.
- Install anti-virus software. Regularly update it and make sure it remains fully operational at all times.
- Use a firewall to prevent unauthorised access to your computer.
- If you use a wireless network, please, make sure your settings are safe. (Do not use WEP encryption; use WPA2 instead; choose a long, random password etc.)
- Use anti-spyware and malware programs (against spy programs or malicious software).
- Only install programs to your computer or mobile device from reliable sources.
- Encrypt any storage attached to your mobile device. Use a screen lock and a password to release the encryption.

Use caution in accessing the e-bank website

- Close all other Internet connections while you are connected to your e-bank
- Type the website's address into the address line instead of clicking on any link received by e-mail. Links inserted into e-mail messages can be easily manipulated, where they may seem to be pointing to the e-bank service, but, in fact, will take you to a different site
- If at the time of connection the browser warns you of a problem with the certificate, do not log onto your e-bank and notify the Bank's Customer Services

- Once you finish your on-line session, always log off e-bank, close your browser and remove the chip card from the reader

Check whether you are truly on the Bank's website

Using the following simple steps you can check whether you are indeed on the Bank's website and have not been redirected to a different website using fraudulent methods:

- Does the address line correctly display the Bank's Internet address, and does it start with 'https'? (Please, note that the difference from the correct address may only be a single letter that is difficult to notice; e.g.: *legjobbank.hu* instead of *Iegjobbank.hu* - capital 'i' instead of lower-case 'L').
- Can you see the closed lock symbol in your Internet browser?
- When you double-click on it, does it correctly display K&H Bank's name and Internet address amongst the certificate's details displayed in the pop-up window?
- For new browser types, are the Bank's name (and the lock icon) displayed in green before the address line?
- Do you experience anything unusual while using the website or logging on to e-bank? Do the usual websites display after log-on?

If not, you may be on a website that is seemingly identical to K&H's, but in fact is a hoax site that was created with the intention of gaining access to your confidential information.

If this is what you **experience**, please, **promptly** notify K&H Bank by e-mail (bank@kh.hu), phone (+36 (1/20/30/70) 335 3355) or in person in any of our branches. Thank you for your co-operation!

Please, use e-bank with caution

- Remove the chip card from the reader when you no longer need it
- When you are finished, log off e-bank, and close your browser
- Request text (sms) messages (Mobilinfo) about all outgoing transactions affecting your account, and if you see any unknown transfer, please, promptly notify the Bank's Customer Services
- Only activate the K&H mobile bank service via the traditional e-bank service if you indeed wish to install and use the mobile application

Get any lost/stolen ID devices blocked by the Bank

- Block any lost/stolen chip cards promptly by getting in touch with the Bank's Customer Services
- If you use text messaging (sms) to log on to the system and your phone gets lost, please, get your SIM card blocked by your telecommunications operator

cégjegyzékszám: Cg. 01-10-041043 nyilvántartó: Fővárosi Törvényszék Cégbírósága

a KBC csoport tagja