Make sure that you are using the original Aareal Portal website.

- When you are working with the Aareal Portal and hover the cursor over the lock symbol in the address line of your browser, a window will appear via which you can view a certificate. You can be sure that you are on Aareal Bank's secure website if the address in the certificate corresponds to the browser address line and if the certificate has been issued for Aareal Bank by an independent certification authority and is still valid.

- The closed lock symbol also tells you that your data is safely encrypted via SSL technology (standard for payments applications). An internet address starting with https:// instead of http:// also means that the website is secured by an SSL certificate.

Aareal Portal

06/2025

CLIENT HOTLINE
(calling to block access to the Aareal Portal or the imageTAN reader, for example)
Phone: +49 611 348 2000
E-mail: kundenhotline@aareal-bank.com

Aareal Bank will never contact you via e-mail, telephone or fax asking you to reveal your personal verification devices, passwords or PINs. The Bank will inform you about the latest security issues via the Aareal Portal.

Aareal
YOUR COMPETITIVE ADVANTAGE.

How-to guide: Secure banking with Aareal Bank's Aareal Portal

Key information to follow when using electronic banking services

Aareal
YOUR COMPETITIVE ADVANTAGE.

Please always follow the advice on this leaflet if you are using our electronic banking services in the Aareal Portal.

Protect your data and passwords, and store your access devices in a safe place.

- To use our electronic banking services via the Aareal Portal, you will need your own device for accessing the portal and releasing payments – i. e. an individualised, encrypted imageTAN reader®, which the Bank will provide. You will also need a PIN, which you can create yourself when activating the account.

- Never write your PIN on the imageTAN reader itself or anywhere on your desk or in file folders that other people might be able to access. Do not share your PIN with anyone.

- Always lock away the imageTAN reader in a safe place once you have completed your banking transactions.

Be sure to block your access right away if you notice any irregularities.

- If you suspect that someone is misusing your access permissions, please contact the Aareal client hotline. Our staff will be happy to advise you on any portal-related security questions you might have. Alternatively, you can ask hotline staff to block your access to the portal or can do so yourself directly via the Aareal Portal, either by blocking your access to the portal or by blocking the EBICS access device itself.

Protect your computer.

- The computer you use to carry out banking transactions via the Aareal Portal must be protected at least by an up-to-date (and ideally self-updating) virus protection software; an additional firewall is recommended. If you work in a more complex hardware landscape, an employee with administrator rights for the individual workstations will usually be responsible for ensuring that malware protection is up to date.

- The existing operating system and browser must always have the providers' most recent security updates installed. Again, this will usually be the responsibility of an administrator.

- Please ensure that access to both the Aareal Bank application and the operating system on your computer is protected, e. g. with a password (you should never use the same password for the portal and your operating system). Lock your computer whenever you leave your workstation.

- Access restrictions and encryptions are required if your computer is connected to the internet via a wireless connection (e. g. Wi-Fi).

Be careful when downloading software and files.

- Malicious software can include viruses or "Trojan horses" that spy on or destroy data on your computer. Only install programs from trusted sources. Unknown image files and links in unsolicited e-mails may also contain malware.