

Më poshtë mund të gjeni disa këshilla dhe udhëzime për të kryer transaksione të sigurta kur përdorni shërbimet E- Banking të Alpha Bank.

### **Kodet e sigurisë së Alpha Web dhe Mobile Banking**

- Zgjidhni kode sigurie të vështira dhe sigurohuni që ti ruani ato në vende të sigurta ku nuk mund të zbulohen nga të tjerë;
- Siguria e kodeve tuaja personale është përgjegjësia juaj. Në rast se ju dyshoni se ju janë vjedhur ju lutemi të informoni Bankën sa më shpejt;
- Mos ruani në të njëjtin vend kodin e përdoruesit dhe kodin e sigurisë pasi nëse zbulohen nga palë të treta, ju i mundësoni atyre aksesin e plotë në llogaritë tuaja;
- Ne rekomandojmë që ju të ndryshoni shpesh kodet tuaja të sigurisë;
- Alpha Bank nuk do t'ju kërkojë kurrë në asnjë mënyrë kodet e sigurisë (psh. telefon ose e-mail). Këto kode janë personale dhe ju nuk duhet t'ia bëni të ditur asnjë njeriu;
- Ekzistojnë e-mail-e dashakeqe të cilat synojnë të zbulojnë kodet tuaja personale. Këto e-mail-e mund të duket sikur dërgohen nga Alpha Bank dhe drejtojnë marrësin drejt linq-eve ku duhet të plotësojnë të dhëna personale (p.sh. kodin e përdoruesit, kodet e sigurisë etj);
- Ekzistojnë telefonata dashakeqe të cilat kryhen nga persona që pretendojnë të jenë staf i Alpha Bank dhe ju kërkojnë të dhëna personale. Këto telefonata ju kërkojnë të zbuloni të dhëna personale si numër llogarie, kod përdorues, numër karte identite, etj.

### **Mbroni kompjuterin tuaj nga veprime dashakeqe**

Ekzistojnë palë të treta të cilat në padijeninë tuaj përpiqen të instalojnë në kompjuterin tuaj , programe dashakeqe (viruse, worms, trojans, spyware, etj), nëpërmjet internetit ose e-mail. Në disa raste këto viruse mund të kapin të dhënat tuaja personale dhe kodet, të shkatërrojnë dokumenta dhe programe në kompjuterin tuaj.

### **Për t'u mbrojtur nga këto veprime dashakeqe Alpha Bank ju sugjeron:**

- Mbroni kompjuterin tuaj me programe sigurie si firewall, antivirus ose antispyware;
- Përditësoni kompjuterin tuaj me versionet më të fundit të sigurisë të sistemit operativ ;
- Fshini dokumentat e përkohshëm të Internetit;
- Shmangni përdorimin e kompjuterave public ose të kompjuterave në palë të treta (p.sh hotele, miq, etj);
- Mos injoroni shenja të "çuditshme" që kompjuteri juaj mund të shfaq, pasi këto mund të shkaktohen nga viruse të instaluara;
- Mos iu përgjigjini kurrë e-maile-ve të cilat kërkojnë të dhëna për llogaritë tuaj ose kode sigurie tuajat dhe mos ndiqni kurrë adresat që ju kërkohen në këto e-mail-e;
- Sigurohuni që ju të aksesoni shërbimet E-Banking vetëm nga kanalet zyrtare të Alpha Bank Albania si faqja e Bankës [www.alphabank.al](http://www.alphabank.al) nga ku mund të aksesoni direkt linkun për të hyrë në e-banking. <https://abaprd.alphabank.al/index/public/model-bank.html?module=login> dhe asnjëherë nga adresa të tjera.

Na kontaktoni në numrin <a href="tel:042278736">042 278 736</a> ose në e-mail <a href="mailto:ebanking.albania@alpha.gr">ebanking.albania@alpha.gr</a> nëse vini re veprimtari të dyshimta në llogarinë tuaj!
---



Below you can find tips and instructions for the protection of your transactions when using the Alpha E-Banking services.

### **Alpha Web and Mobile Banking security codes**

- Choose complex passwords and keep them in a way that will ensure that their disclosure or theft is not possible
- Keeping your personal security codes safe is your responsibility. In the event of a confirmed or suspected physical or electronic theft, you must notify the Bank immediately
- Do not keep your User ID and Password together. If they are leaked to third parties, they will gain access to the system and to your accounts
- We recommend that you change your Password at regular intervals
- Alpha Bank will never ask you for your security codes in any way (e.g. via phone or e-mail). They are personal and you must not disclose them to anyone
- Misleading e-mail messages (phishing emails) aim to intercept your personal data. These messages are supposedly sent by Alpha Bank and urge the recipient to follow a link to a particular page in order to enter his / her personal data (e.g. User ID, Password, Additional Password etc.)
- Misleading phone calls (voice phishing) by persons claiming to be Alpha Bank representatives aim to intercept your personal data. These phone calls urge the user to disclose his personal data (e.g. Account Number, User ID, Tax Registration Number, and Identity Card Number etc.).

### **Protect your computer against malicious acts**

Many malicious third parties try to install to your computer, unbeknownst to you, malicious software (Viruses, Worms, Trojan Horses, and Spyware etc.) via the Internet or by e-mail. In some cases, this malware could intercept your personal data and codes, destroy your files and programmes and generally harm your computer.

### **Alpha Bank informs you about the risks of using electronic systems and, in order to help you carry out your electronic transactions securely, suggests that you:**

- Shield your computer with security software, such as Firewalls, Antivirus, Antispyware;
- Update your computer with the latest versions and security patches of the operating system, the anti-malware programs and the browsers that you use;
- Delete the temporary Internet files from your computer;
- Avoid using public computers or those belonging to third parties (e.g. hotels, your friends);
- Do not ignore "strange" behaviors of your computer, as these may be caused by installed malware;
- Do not reply to e-mails that ask for your account details or security codes and do not follow the links that they suggest;
- Make sure that you visit the E-services of Alpha Bank through the official channels of the Bank such as through the official website [www.alphabank.al](http://www.alphabank.al) where you can access the e-banking at <https://abaprd.alphabank.al/index/public/model-bank.html?module=login> and never use other websites or links.

Contact us at the number [042 278 736](tel:042278736) or at the e-mail [ebanking.albania@alpha.gr](mailto:ebanking.albania@alpha.gr) if you notice suspicious activity in your accounts