# Internet Banking Security Statement

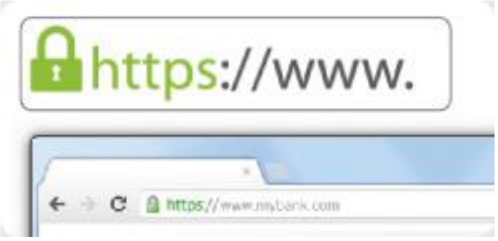
Online banking is a very secure and convenient way to access your bank's services. However, you need to be wary of fraudsters trying to gain access to your account. This is usually done by illegally obtain you credentials such as your username, passwords, or your memorable information (for example PIN codes, secret questions)

## How to use Internet Banking Safely

**Here are some essential tips:**

- Never login to your bank website clicking on link in an email, even if an email message looks like email from you bank. Always type internet banking web address by yourself, tying it directly into your browser.

- The login pages of internet banking web site is secured through an encryption, meaning that a locked padlock or unbroken key symbol should appear in your browser window when accessing protected site. The beginning of your bank's internet address will change from 'http' to 'https' when a secure connection is made.



- Be wary of any unexpected or suspicious pop-up windows that appear during your online banking session.

- Never share your login details even partially either by email or over the phone. Remember that FINCA bank never ask clients to share confidential information in this way.

- Fraudsters sometimes try to trick people into conducting a real payment by claiming "it's just a test". Remember, FINCA never requests its clients conduct "test" transactions

- Check your bank statements regularly. If you spot any unauthorized transaction, contact your bank immediately.

- When transferring money via internet or mobile banking, double check the amount and destination account well.

- Install and regularly update antivirus on your personal computer and mobile device. Regularly update OS and all installed software. Try to setup your browsers security settings properly. Details are here: https://www.us-cert.gov/publications/securing-your-web-browser#why

- Different banks use different approaches to prove identity of internet or mobile banking users. FINCA Bank Georgia uses one-time SMS codes. In order to approve particular type of transaction you have to enter SMS code, which you receive from FINCA on your mobile device. This is also known as two factor authentication (2FA). SMS codes used as one of the security steps to authorize a payment. Never use codes received from sender others then FINCA.

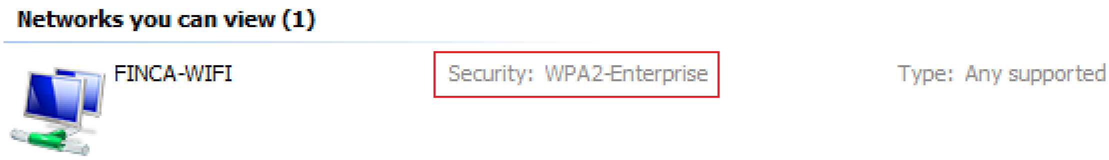
- Make sure that FINCA has always the last information regarding your phone number and contact details in general. It is preferable to use phone, which is under your ownership.

## Public Wi-Fi hotspots.

Both, in case of Internet Banking and Mobile banking, particular attention should be paid to Wi-Fi network security. Public Wi-Fi spots are a very convenient way to access the internet. However public Wi-Fi spots could be very risky. Accessing your online banking services over an unsecured public Wi-Fi spot is not recommended.

**However if there is no other choice, here are some simple measures that you can take to stay safe when using public Wi-Fi:**

- **At least try to pick the most secure network.** Wi-Fi security settings can vary, if you have a choice it is recommended connect to the one with the highest security settings such as WPA2, followed by WAP and then WEP. After connecting to public Wi-Fi, set your operating systems network location to a 'Public Network'. Your operating system may prompt you with a pop-up that has the option to do this. This security feature blocks others from accessing your files and other areas of your device.



Networks you can view (1)

FINCA-WIFI

Security: WPA2-Enterprise

Type: Any supported

- **Use a Virtual Private Network (VPN).** If you are regular user of public Wi-Fi, consider using a VPN as from personal computer as when using mobile device. VPN creates a secure connection/tunnel between your computer and the internet. It will prevent others from potentially snooping and intercepting your communication to a website and stealing your credentials (username and password). There are a number of free and commercial VPN products available.