INSTRUCTIONS FOR ONLINE PURCHASES

1. Diversify the portfolio of your bank accounts – If you buy online frequently, it is important to ensure that your money is not lost from cyber fraud by diversifying your account connected with your card. The best thing is to keep two accounts, one for purchases on the internet (linked to the card) and the second one is an elastic deposit or current account. In the account that you use for online purchases you can transfer funds from the second account through e-banking / Mobile Banking. Just make sure you transfer the amount you need to make the purchase. This will minimize the risk of stolen card data during the transaction.

2. Online purchase limit – In order to minimize the risk, do not keep a high limit for online shopping. You can keep a limit that you find reasonable for the transactions you want to perform. If you need a higher limit, you can increase it, which will expire after the date you have set.

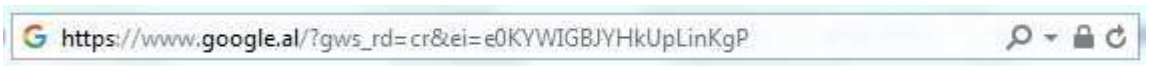
3. SMS banking – All the customers who purchase online should be provided with SMS banking and will be notified by an SMS for all their card transactions. If the client does not recognize the transaction that is sent via SMS, he/she should immediately notify the bank to block the card until the client gives the final confirmation after identifying the transaction. This service prevents in a timely manner all the cases where the card data become vulnerable and could be stolen as well as the attempt to be use these data on different pages, by blocking the card any unauthorized actions cannot be carried out.

QUALITY SERVICE CENTER
0800 48 48 (toll free)

Monday – Saturday 09:00 – 19:00
+355 (0)68 40 12121; +355 (0)69 40 12121

4. Choose trustful websites – In general, big websites which you might have heard of are considered safe. This is one of the reasons why sites such as Amazon, Ebay and other sites dominate sales on days like Black Friday (this is the day with the highest sales of the year). If you have already purchased on these sites once and are satisfied with the security level they offer, you can use them again for your purchase.

5. Purchase only from encrypted sites (safe sites) – check the web address. Is the page you are buying from safe? Try to avoid public computers during purchasing. Most of the browsers will display their safety information in their page. If the HTTPS will be displayed in the web address, this means that the page is encrypted. If a browser detects an unsafe connection this means that the page is not encrypted and unauthorized people (hackers) can steal your data transmitted in this page. Most of the browsers have a lock symbol when they are safe. If this symbol is missing, the page is not safe and can be of a high risk to purchase from it.



OTP Bank Albania
Twin Towers
Bul. "Dëshmorët e Kombit"
Kulla 1, Kati 9
Tirana, Albania
Tel. +355 4 2 280 442/3
Mob. +355 68(69) 40 12 121
www.otpbank.al

6. Delete your online presence – If you do not need an account on a merchant site anymore then delete it. Keeping your data across several merchant accounts is a good invitation for theft / loss, especially when you do not remember who owns your data and for what purpose it will be used.

7. Check your online accounts often – If a fraud has occurred, the quickest way quick to detect it is to check your online accounts daily (eg your account on PayPal). Especially if you are a frequent buyer online or during vacation period in which the number of purchases increases. A quick search on Google with the name of the page followed by the word "hack" can help you identify if certain pages that you use often have been attacked lately.

In addition, check continuously your card account so that you might identify transactions that have not been authorized by you.

8. Do not visit any website without identifying it first – Web pages that are not familiar carry a higher risk for fraud. Over 40,000 fake sites that used to sell web apps have been shut down by the authorities. Nobody would want to be part of their scams.

Verify the identity of the page you will be purchasing from by using the link below:
http://www.scamadviser.com/

9. Use safe passwords – Many sites will push you to create a secure password, but it is best to select a password even on those pages that this is not mandatory. It is easy to select a secure password, the more characters the password has the safest it is (at least 8 characters). Do not just use capital letters, use also numbers and punctuation.

10. Do not use the same password twice – Sometimes it can be quite annoying to try and remember all the passwords that you use in different sites but programs like iCloud Keychain and 1Password will help you do just that. This programs keep your passwords encrypted and safe by making it easier to navigate through the pages you have been registered.

11. Avoid spam – They can be a good phishing method. These offers might be difficult to be identified as dangerous and they can simply deceive you to collect your data. If you are in doubt, contact the vendor by using the official data given in their official website to verify the content of their e-mail. If you receive an e-mail requesting to give out the data of your card you must never reply to it.

12. Be careful with the addresses – If you must click an internet address from your e-mail, just place the mouse over it (without clicking) in order to understand where this address will lead you. Do not click on addresses without knowing the page it will land you on, unsafe pages might install an undesired software in your computer and steal your data.

OTP Bank Albania
Twin Towers
Bul. "Dëshmorët e Kombit"
Kulla 1, Kati 9
Tirana, Albania
Tel. +355 4 2 280 442/3
Mob. +355 68(69) 40 12 121
www.otpbank.al

13. Avoid online gifts – as good as it might sound to receive a gift such as a Macbook from an online page, it is probably a fake one. In fact, data from ACI worldwide show that offers from virtual gifts (Gift Cards) have a high probability to be hacked. An example below:

14. Avoid clicking on advertisements – Many fake ads might install malware (a software which might damage your computer) in your computer and might log in to your accounts and pass your personal data to unauthorized persons to use them. Do not click on ads if you are not fully certain on their origin, especially when they appear on sites that you do not trust.

15. Never complete a purchase over public Wi-Fi – Especially for safe transactions. You are never fully aware you might be observing. Fraud experts come up every day with new ways to overpass security. Using a hotspot (Wi-Fi) which you do not have control on, is considered bad practice.

16. Use PayPal if you can – If an internet page gives you the possibility to pay with PayPal use it, it's safer. According to PayPal, your data is much safer when it's used through this financial intermediator, because it offers state of the art encryption technology.

OTP Bank Albania
Twin Towers
Bul. "Dëshmorët e Kombit"
Kulla 1, Kati 9
Tirana, Albania
Tel. +355 4 2 280 442/3
Mob. +355 68(69) 40 12 121
www.otpbank.al