

## Security Disclosure

Last Updated: August 2018

At Denizen we are aware of the need to ensure the transit of information with people interested in our activities. That is why Denizen places great emphasis on security and the confidentiality of all communications. Transactions are made using a secure server with the SSL (Secure Socket Layer) protocol, which is activated when the service is accessed. The secure server establishes a secure connection that transmits encrypted information using algorithms, thereby ensuring it can only be read by the customer's computer and the bank's server. So using the SSL protocol provides:

- That users communicate their data to the Denizen server and not to any other server purporting to be Denizen.
- That the purchasing data is transmitted in encrypted form between the user and the Denizen server center.

## Security in Your Passwords

Denizen uses a system of **Secure Passwords**.

Your Denizen card PIN number and your access code to the Denizen app are private information that must be securely safeguarded. They are stored in our internal systems and encrypted so no one at Denizen knows them.

Denizen will never ask you for your Denizen credentials by e-mail, telephone or SMS. If you receive this type of message, please do not provide any information. Passwords are secret and should be known only to their owner for their exclusive use on Denizen app.

Browsers offer the option of saving the usernames and passwords for the websites that require them, which are then stored in your computer's memory. This practice, although it speeds up access to sites requiring a username and password, is totally inadvisable in the case of passwords for banks or other services which could cause serious damage to the users in the event of loss or theft.

Denizen recommends never saving your access codes to our application on a computer or tablet. These devices may be the object of computer attacks and your codes could be exposed.

## Tips

- Use complex passwords that are difficult to guess and contain a mix of lowercase and uppercase characters and numbers.
- Don't share your passwords with anyone. Passwords are secret and should be known only to their owner.
- Don't write your password down on post-it notes or in notebooks; memorize it or use specialized password managers.
- Disable the "save password" option on your browser. It's safer to enter it each time you log on.
- Change your passwords periodically.
- The PIN and the access code must be different. This will make it more difficult for a third party to discover or guess them.

- If you suspect that someone has been able to guess your access code you should change it as soon as possible.

If you receive an SMS confirming a transaction you haven't made, contact Denizen at [support@denizen.io](mailto:support@denizen.io).

## Detecting Attacks and Viruses

Computer viruses are programs whose purpose is to install themselves in a computer without user's permission or knowledge. There are several types of viruses, but all of them tend to share the property of propagating and spreading in the computer itself via the Internet.

It's easy to inadvertently contribute to spreading viruses by resending e-mails containing infected attachments. The collaboration of all Internet users is essential to avoid the spread of computer viruses.

There are different types of virus, of which some of the most notable are:

- **Phishing:** This consists of sending an e-mail purporting to be from a well-known organization and requesting the user's data (address, bank details, passwords, etc.). To provide this data, the user is in most cases required to follow a link that appears in the e-mail and then enter the requested information once on the bogus page.
- **Ransomware:** This is a lucrative method of technological delinquency. Usually concealed as "parcel delivery services" or any other credible excuse, it is propagated via email with links that enable the installation of programs or the download of infected files. This virus blocks access to computer information and demands a ransom that will supposedly provide the key to decrypt the information.
- **Trojans:** These are introduced into personal computers embedded within a program. They transform the computer's behavior so that everything that's done on it can be seen from the delinquent's computer.
- **Hoaxes:** These are emails conveying certain false rumors with the sole aim of transmitting and increasing the low-quality information circulating on the Internet. They are generally not very harmful, and are easy to eliminate.

The following is a list of the main symptoms that can be observed in a computer infected by a computer virus:

- Operations are performed more slowly.
- Programs take longer to run and load.
- There is an occasional or permanent and unexplained reduction in the free space on the hard disk and the available RAM memory.
- Unfamiliar programs may appear in the memory.

## Tips

Below is a list of precautions you should take to increase your security against viruses:

- If you have to enter your credentials, check that the address (URL) of the server begins with https, which means you are accessing a secure server.
- Another indication that the server is secure is the presence of a closed padlock (as opposed to an open one in the case of a non-secure server) to the left or right of the address (URL).
- Check the security certificates of the page you are on by clicking on the padlock icon that appears when accessing a secure area, or on the certificate in the browser bar, and check

- that the expiry date and domain of the certificate are up to date. The detailed information includes the issuer, the period of validity and who the certificate was issued to.
- Before clicking on a link, move the cursor over it to see the address you'll access when you click on it. Check that the address is correct and is related to the activity you want to carry out.
  - Whenever you finish a transaction or query, remember to use the log-off button. This will securely end the session at Denizen app, and the next time you log on, you'll be asked for your user number and access code again.
  - Your operating system, your browser and extended use programs must always be up to date.
  - You should install a firewall and antivirus program and always keep them updated and running.
  - It is advisable to make regular backup copies of your files.
  - Don't connect any external device to your devices if you don't know where it came from, such as flash drives, hard drives and unknown cellphones.
  - Download programs and apps only from official websites.
  - Set an unblocking pattern on your devices so they can't be accessed by third-parties.

## Cards and eCommerce

Denizen takes card security seriously. Security in queries and operations via the Denizen app is based on a system of secure codes. These are saved in our systems and encrypted with an algorithm so no one at Denizen knows these codes. The Denizen app allows you to turn your cards on and off easily.

### Tips

Denizen recommends following these tips to increase the security in the use of your cards:

- The card must be signed and is absolutely personal and non-transferable.
- Memorize your secret number. Never write it down or tell anyone under any circumstance.
- Don't use personal data in your secret number that can be easily deduced, like your date of birth or your license plate
- Destroy expired cards with scissors; don't just throw them away without destroying them.
- Be alert to the expiry date of your Denizen card. If you don't receive a new card, immediately notify Denizen to [support@denizen.io](mailto:support@denizen.io)
- When you make a purchase, don't lose sight of your card and ensure it is returned to you. Keep a copy of the transaction slip and compare the charges shown on the statement.
- Immediately report the disappearance of the card by calling to +1-844-207-7702 or through the app in Card management menu tapping "Report card as lost or stolen" button. The speed with which you do this is crucial.
- Before setting out on a trip, check the card's expiry date and your credit limit.
- Make a note of the number +1-844-207-7702 so you can contact us in case of any problem with the card.