Security Policy

Security Information

NinjaCard® has strict policies and procedures in place to maintain stable and secure systems for the protection of customer information. The security of personal information is a collaboration between NinjaCard® and you, our customer. This security page was developed to provide our customers with the information necessary to protect themselves and their computer systems from fraudulent activity. Should you have any questions or concerns, we encourage you to contact the NinjaCard® Service Center toll-free at (855) 646-5242 or by email at support@ninjacard.com.

Security Alerts

For your protection, all PIN-based transactions are permitted within the US.

If you experience any difficulty using your debit card, please call us at (855) 646-5242.

Fraud & Theft

Theft - How to protect yourself from Theft

- Set up real-time financial alerts to monitor your finances.
- Purchase or utilize a paper shredder, and shred anything containing sensitive information.
- Limit the information you release, especially online, or with foreign entities.
- Trust your instincts. If it seems suspicious, it likely is. Be sure to web search any suspicious or unknown phone numbers and or emails to identify any reported fraud.
- Monitor your credit reporting activity.
- Create strong and secure passwords – utilize the highest level of authentication possible.
- Limit what personal information you post on social media. Hackers and phishers will follow you on social media to determine when the best time to compromise your information would be.

If you have any concerns about theft please reach out to the Service Center for immediate assistance.

Useful Links for Identifying and Preventing Fraud

https://www.fdic.gov/consumers/consumer/news/january2019.html?source=govdelivery&utm_medium=email&utm_source=govdelivery

https://www.consumer.ftc.gov/blog/2018/09/your-social-security-number-isnt-suspended-ever

https://www.consumer.ftc.gov/articles/0048-government-imposter-scams

https://www.fdic.gov/consumers/consumer/news/cnsum18/scams.html

https://www.fdic.gov/news/news/press/2004/pr9304b.pdf

Phishing

Phishing is an Internet-based scam that uses email to deceive customers into disclosing sensitive information such as credit card numbers, account numbers, social security numbers, PINs, and passwords. Fraudsters tell the recipient that they need to "update" or "validate" information. Phishers have become very creative at appearing legitimate. Typically they provide a link within the email that redirects the user to what appears to be a legitimate website, but actually, it is a website they have designed to steal information. Even the savviest Internet user has been tricked by a phishing scam.

Always Remember

- Never provide sensitive information such as your Social Security Number, passwords, PINs, or account numbers via email as NinjaCard® will never request this information via email.
- Never click on an embedded link that requests sensitive information

NinjaCard® does not request information in this manner.

- Report suspicious activity immediately

Call the Service Center at once if you feel you have been the victim of a phishing scam

Online Banking Security

How to keep your Personal Information safe

- Never fall victim to relinquishing your User ID and password for any online accounts.
- Ensure that all email communication is secure or encrypted to protect your information.
- Ensure that you have the latest system security updates and patches applied to your mobile device or computer.
- If you receive an SMS (Text) message that you do not recognize, do not respond.

- Bookmark the NinjaCard® webpage – NinjaCard.com - and access the site only through your bookmarks to avoid any phishing sites.
- Keep away from utilizing unsecured public Wi-Fi.
- Monitor your accounts online regularly. Be sure to notify the NinjaCard® Service Center Immediately if you identify suspicious activity.
- Use only your cellular network when facilitating mobile financial services and transactions.
- Disable automatic logins for any and all online accounts that hackers could mine information from.

Computer Security

It is very important to follow good security practices to prevent home or office computers from being compromised. Two of the biggest concerns for computer users today are viruses and spyware. In both cases, you can defend yourself against them easily enough with just a little bit of planning:

- Install and use anti-spyware software to scan for adware and spyware that may be installed on your computer. There are many products available.
- Keep your computer's software patched and current. Both your operating system and your anti-virus application must be updated on a regular basis.
- Only download software and updates from reputable sources. For operating systems, always go to the legitimate websites of the company or person who produces them (i.e. Microsoft or Apple).
- Always think before you install something, weigh the risks and benefits, and be aware of the fine print. Does the lengthy license agreement that you don't want to read conceal a warning that you are about to install spyware?
- Install and use a firewall.

Things to avoid:

- Never open an email attachment if you are unsure of the source. Delete it immediately.
- Never download any application or executable files from an unknown source and be careful when trading files with other users.
- Be cautious of "Pop-up" Ads. A good rule of thumb is to close pop-up ads by clicking the "X" close option in the upper right-hand corner. Even the "Close" or "Cancel" buttons have the ability to install malicious programs.

Email Security

Although email has become our society's standard for communication, you must be aware that it is not secure. You should never include sensitive information such as your Social Security Number, passwords, PINs, or account numbers via email.

We suggest you use only the last four digits of an account number if you need to correspond via email. It is also helpful to provide a daytime telephone number in your correspondence so that we may contact you.

ATM Precautions

When utilizing an ATM it is very important to remain alert, and follow the below suggestions:

- Prepare all transactions at home
- Never lend out your card or card information.
- Survey that area around where you are about to make the transaction, especially if it's after dusk.
- Keep a transaction record book, and balance your accounts regularly. For best practice keep all ATM receipts for proof of deposit/withdrawal.
- Use your body as a shield to prevent others from viewing your PIN when entering it into the ATM or POS system.
- Be SURE to remove your card from the ATM upon completion of your transaction.
- Be SURE that you have not forgotten any documents at the ATM vestibule.
- Be discreet about making cash visible both approaching the ATM and leaving the ATM.
- Do NOT accept assistance from anyone while using the ATM or night depository.

Security Support

If you have any security concerns please feel free to reach out to our Service Center for great customer service and assistance with your issue(s). The Service Center can be reached toll-free at (855) 646-5242 or by email at support@ninjacard.com.