Internet Banking Security Tokens FAQs

jcbank
JACKSON COUNTY BANK
MEMBER FDIC
8 Main St., P.O. Box 490, Black River Falls, WI 54615
jacksoncountybank.com (715) 284-5341

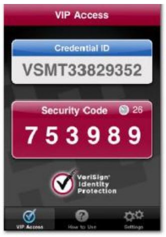
What is a Security Token?

Security Tokens are devices that help authenticate users. They emit constantly changing "passcodes" that users enter during login. When a user enters a Security Token passcode along with their user ID/password, they meet the multifactor authentication requirements for "something you know" and "something you have" in a very literal way.

Security Token Devices available:

A Physical token is a hardware that you maintain in a secure location at the office.

A virtual token is software you download to a mobile device.



Your business needs will determine which type of token to select. Once you elect to utilize the Security Token you will be required at every login to enter the passcode generated by the token in addition to your User ID and Password. For some businesses that only utilize Internet Banking at one office location, a physical token may be the best choice. However, for a business user that may utilize Internet Banking from different terminals (computer in the office, laptop at home or with mobile device while traveling) the virtual token installed on your mobile phone may be a better solution.

Token Security Recommendations and Best Practices:

- All tokens should be stored securely
- Keep the serial number or credential ID of the token confidential
- Enforce strong password policies
- Do not provide user names or other credentials to anyone without verifying that person's identity
- Update security products and operating systems with the latest patches.

Why Tokens? Why Now?

Malicious Virtual programs, called "malware", represent the greatest threat to online financial applications today. This is especially true of "trojans", programs that hide on a user's computer in order to steal confidential information. Malware can infect a user's computer through illicit email attachments or rogue websites. Once they gain a foothold, these programs monitor the sites a user visits and the keystrokes they enter. Their goal is to capture online financial application credentials. Infected machines can provide cyber-thieves with user IDs, passwords, and even the answers to security challenge questions. Security tokens defeat malware programs by generating a new passcode every few minutes. Users must enter the current passcode to access the system. Even if malicious programs capture stolen credentials, the token passcode expires within minutes. Since only the user who has the token can know the current passcode, cyber-thieves are prevented from accessing the system. The number of computers infected by malware is growing dramatically. Incorporating tokens as an authentication tool is a recommended step in further protecting your online banking session.

In today's online world, the landscape of ever-evolving security threats demands greater defenses. Jackson County Bank is committed to providing security to meet these needs, however maintaining the integrity of your computers is ultimately your responsibility. The time and effort to maintain a secure computer seems minimal compared to the physical loss of dollars that may occur as a result of a malware or phishing attack on an unprotected computer.

Can tokens be used simultaneously by the same customer?

Tokens are assigned based on the Internet Banking User ID and therefore only one token may be utilized. However if you have more than one Internet Banking User ID you may choose to have a Virtual token for one User ID and a Physical token for a separate User ID.

What happens when a token expires?

Physical tokens are guaranteed for three years, but may last for five years. A new token will be issued to you at the end of the third year. Virtual tokens do not have an expiration date.

Can I use a token with my Tablet?

Physical tokens may be used with a Tablet or PC however Jackson County Bank does not currently support the installation of a Virtual token on a Tablet at this time. Virtual tokens may be used with a mobile phone.

Once I receive my token, what do I do next?

Once you have received your Physical token from Jackson County Bank or have downloaded your virtual token you will be required to register the token. The token registration is completed by logging into Internet Banking and submitting the token serial number and token code. Once you have successfully completed the registration process you will be required to enter your token code at each Internet Banking login after the correct User ID and password are accepted.

How long do I have to register my token?

You should register your token within ten days of receiving the Physical token or successfully downloading the Virtual token. If you do not complete the registration process within the next ten days you will be required to contact Jackson County Bank at 715-284-5341 to have the registration period extended.

Will my token be locked out if I enter the incorrect token code?

Yes. The token will need to be reset after ten invalid attempts. Please contact Jackson County Bank for assistance at 715-284-5341.

What is a Credential ID?

A Credential ID is also referred to as the token serial number in the case of a Physical or Virtual token.

Can a Virtual token be installed on more than one device?

No. Virtual tokens have a unique Credential ID that cannot be redownloaded.

Can multiple Virtual tokens be installed on a single device?

Yes. You can have a Virtual token on your mobile phone for your business Internet Banking and you may also have a separate Virtual token for your personal Internet Banking on the same mobile phone.

Is there a charge to download the Virtual token?

There is no charge from Jackson County Bank to download the Virtual token however carrier charges may apply from your mobile provider for download and activation. A mobile data plan with Internet access is required.

Is there a fee from Jackson County Bank for using a Virtual or Physical token?

No. Please refer to the Bill Pay Cycle Fee area of the Services and Fees Brochure.

If my phone is lost or stolen, can the Virtual token be used by someone else to access my Internet Banking?

No. You cannot use a Virtual token alone to access your Internet Banking account. A Virtual token is used with your User ID and password, and only you know your password(s) to access Internet Banking.

Can I transfer a Virtual token to another phone?

No. You cannot transfer a Virtual token to another phone. If you have a new phone you will need to download a new Virtual token.

How do I download a Virtual Token to my iPhone® or iPod touch®?

You can choose either of the following options:

- Download from the Apple® App Store by searching the Business category for "VIP Access"
- Download from iTunes and sync your iPhone or iPod touch

How do I download a Virtual token to my Android™ phone?

Choose one of these three options:

1. *Download from your phone's default browser:*
   Enter **m.vip.symantec.com** and follow the installation prompts.
2. *Download from Android Market:*
   Search for *VIP Access* in the Android Market from your phone.
3. *Download by sending a text message to your phone:*
   - Select your country from the drop-down list.
   - Enter your phone number.
   - After receiving a text message, open the URL.
   - Open the download link.

How do I download a Virtual token to my Windows Mobile® phone?

Choose one of these three options:

1. *Download from your phone's default browser:*
   Enter **m.vip.symantec.com** and follow the installation prompts.
2. *Download to your desktop:*
   - Click the Instructions link.
   - Follow the download instructions to sync your desktop to your phone.
   - Copy the VIP Access .cab file from your desktop to your phone.
3. *Download by sending a text message to your phone:*
   - Select your country from the drop-down list.
   - Enter your phone number.
   - After receiving a text message, open the URL.
   - Open the download link.

Internet Banking Security Token Frequently Asked Questions

How do I download a Virtual token to my BlackBerry® or to other supported phones?

Choose one of these two options:

1. *Download from your phone's default browser:*
   Enter **m.vip.symantec.com** and follow the installation prompts.
2. *Download by sending a text message to your phone:*
   - Select your country from the drop-down list.
   - Enter your phone number.
   - After receiving a text message, open the URL.
   - Open the download link

Once I've downloaded the Virtual token, what do I do next?

For security purposes, the token will need to be registered with the Credential ID and token code. This is completed upon logging into Internet Banking.

How do I terminate my Virtual or Physical token use?

If you wish to terminate the use of your Virtual or Physical token you will be required to sign an Opt Out Waiver. If you are utilizing a Physical Token, you will be required to return the token to the Jackson County Bank, P.O. Box 490 Black River Falls, WI 54615 ATTN: Accounting Department. Once the waiver and token have been received Jackson County Bank will terminate the token requirement from your Internet Banking application. If you are utilizing a Virtual Token, you will be required to complete the waiver and uninstall the Virtual Token. Contact your mobile phone carrier for instructions for uninstalling the Virtual Token. Contact us at 715-284-5341 with questions on terminating use of the token.

What do I do if my Physical token is lost or stolen?

Please contact Jackson County Bank immediately if your Physical token is lost or stolen at 715-284-5341.

What do I do if I believe my Virtual token is compromised?

Please contact Jackson County Bank immediately if your Virtual token has been compromised at 715-284-5341.

What are the best practices for token security?

- All tokens should be stored securely
- Keep the token serial number or credential ID confidential
- Enforce strong password policies
- Do not provide user names or other credentials to anyone without verifying that person’s identity
- Update security products and operating systems with the latest patches

How do I contact the bank for support or information regarding Security tokens?

If you have questions or concerns regarding your Security Token please contact us at 715-284-5341.