Account Takeover Alert: Detect Potential Malware or Virus

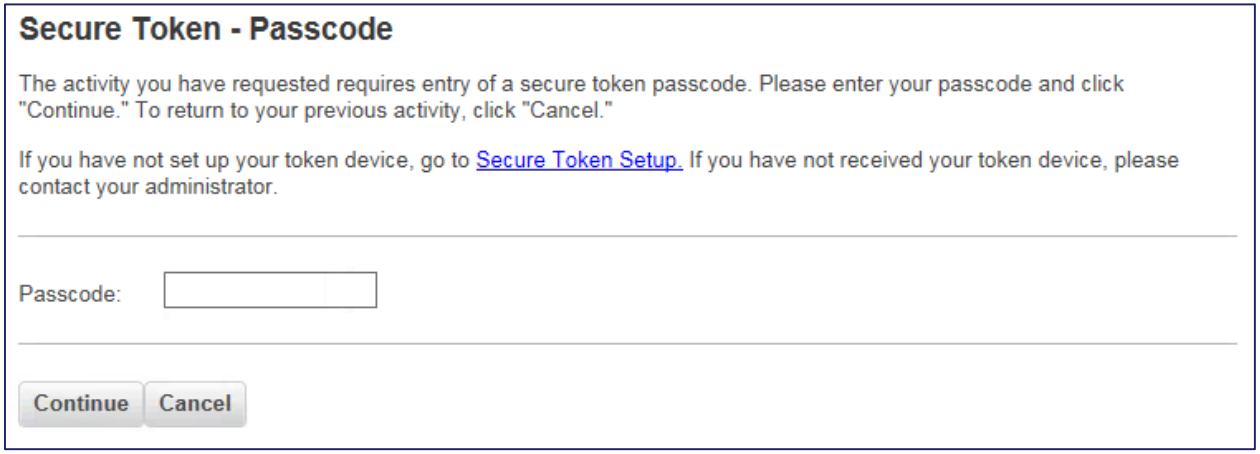
This communication specifically focuses on malware and viruses and tips on how to detect an infection in your device, perpetrated by a fraudster, intending to access your online banking and potentially steal money. This situation is commonly referred to as Account Takeover.

The number one indicator of an Account Takeover is unfamiliar pop ups on what appears to be your EagleBank online banking page. The fraudster will create pop up messages asking for information, such as:
Your login information.
Your personal information – social security number, date of birth, etc.
Your token code from your token or your token PIN or maybe just PIN.

Or after signing on, a message pops up asking you to wait due to technical difficulties or system issues.

EagleBank will never present you with a pop up to ask for information or ask you to wait.

The only time you are presented with a pop up like screen asking for information is after you select the “transmit” button when approving a wire or ACH transaction. This pop up is displayed below and will never deviate. This pop up is the only legitimate pop up from EagleBank.



Account Takeover Alert: Detect Potential Malware or Virus

Other signs that your device may have an infection are:

- Your Internet browser is exhibiting strange behavior
- Home page has changed
- New tool bar appears
- Constantly freezes or is unresponsive
- Internet searches (Google) display inaccurate responses or always take you to the same sites when clicking on a search response link
- Overall slowness at start up, when opening files, or on websites
- Security or anti virus programs disabled
- Unfamiliar error messages
- Can't access admin functionality (control panel, task manager, command prompt, etc.)

Help yourself avoid infections by doing the following:

- Use a firewall
- Install antivirus software
- Make sure you are using the latest version of software (windows, iOS, etc.)
- Adjust your browser security settings
- Do not click on links unless verified as legitimate ahead of time
- Avoid internet browsing, social media, and email programs on computers used for online banking access.

For more information:

For Windows visit: https://www.microsoft.com/en-us/security/?rtc=1

For MAC visit: https://www.apple.com/macos/security/