

National Bank

SECURITY ALERT



New Computer Virus May Prompt Online Fraud Attempt

Please be on the look out for a new computer virus that may be on your computer. This virus may cause a fraudulent screen to appear in the online Bill Payment window. The screen posts messages that attempt to trick you into providing sensitive information such as your account numbers and passwords – information the bill payment system already knows and you should not provide again.

If you are using online Bill Payment and a new screen appears out of context asking you to provide sensitive information, **do not provide this information.**

If you're in doubt about the validity of a screen, please call customer service.

New Security Threat

A new computer virus has been identified that may cause a fraudulent message to display on an end user's computer while they are in the process of paying their bills online. This message attempts to trick users into providing sensitive information such as account numbers and passwords in order to commit fraud.

The fraudulent message is generated from a source outside of National Bank's system, but an end user may be impacted if they have unknowingly infected their computer with the new virus through activities such as illegally trading software, executing files sent via email, or allowing scripts to execute while browsing the Internet.

When an end user whose computer is infected with this virus is using online bill payment, the virus may intercept the browser session and display a fraudulent Web page to the user requesting additional information. This fraudulent Web page appears framed within the bill payment window and prompts the user for sensitive information such as debit card account numbers and passwords. This is an attempt to commit fraud, and the user should not provide the requested information.

National Bank and our bill payment provider partners would never ask an end user for this information in the middle of a bill payment transaction. Any deviations from the documented and expected bill pay system behavior may be attempts to commit fraud.

Again, this particular fraud attempt would only occur if an end user has the virus on their local computer since the fraud attempt is taking place in a browser window that is outside of the National Bank Internet Banking system.

Best Practices for Online Security

To help prevent fraud end users should:

1. Only install software from trusted sources and known origins. Software sent via email is particularly dangerous as viruses are often transmitted via email.
2. Install and maintain Antivirus and Anti-Spyware software on your computer.
3. Update browser software to benefit from the latest security protections.
4. Pay attention to warning messages presented through your browser. Browser warning messages may indicate a security threat.