Don't Fall Into the Malware Trap

First National Bank works hard to protect and secure your Online Banking service and to educate our customers of the importance of the safety of their Online Banking service. As a customer, you play a key role in keeping your information protected. Together, we can make your Online Banking service a secure and safe environment.

Throughout the Community of Online Banking at many banks an increase of malware activity with a screen takeover, targeting token users, has been detected. This particular malware will prompt a user to input account and/or token data, which then results in another screen prompt indicating that the user will be unable to access the account for 24-hours while maintenance is performed. This allows the fraudster to take over the session and commit fraud while the user is detained on the fake "maintenance" screen.

A similar option of the malware has been identified where the customer receives a pop up asking for several pieces of personal information including a phone number. The customer inputs the data and then receives a phone call immediately from a caller claiming to be a bank employee letting them know the system will be down for 24-hours which then allows the fraudster to access the account while on the phone with the user.

First National Bank performs Online Banking Maintenance periodically. The user will be notified with a warning message 24-36 hours prior to the actual maintenance after logging into Online Banking.

Users who are infected should immediately conduct an anti-virus scan. Contact Customer Support at (479) 788-4237 immediately before entering account or token information on new or unfamiliar screens.

Unfamiliar Screen Examples