Safe Mobile Banking Practices

At Lafayette Schools Credit Union, we are committed to ensuring that your account information is safe. It is important that you help protect your mobile devices, computer and account information, too. Here are tips to help you.

Create a Secure Mobile Device

- **Use strong passwords**
  This includes the password to access your mobile device and the passwords for applications within it. Use a combination of upper and lower case letters, numbers, and symbols. Don't share your passwords.
- **Use security software**
  Protect your mobile device just like a computer. Check your device settings for installed security features and determine if you need to make them active.
- **Don't modify your phone**
  Overriding or defeating security or other limitations placed on your mobile device can disable security features making your device vulnerable to malware, viruses, Trojans and other malicious software.
- **Report a lost or stolen device**
  Your carrier can deactivate your device. Login to Online Banking to deactivate your mobile banking account or contact us for assistance.

Operate Your Mobile Device Securely

- **Only download apps that are signed and are from a trusted source**
  Before you download, research the app and make sure you know what it does, what information it accesses (i.e. contacts) and what permissions it wants.
- **Don't open unexpected attachments**
  Opening files attached to emails can be dangerous, especially when they are from someone you don't know, since they can allow harmful viruses.

Keep Mobile Banking Activity Secure

- **Keep Bluetooth turned off when conducting mobile banking activity**
  An active Bluetooth connection could allow others near you to collect data without your knowledge.
- **Use a secure network**
  Use your cellular network or a known secure Wi-Fi network when using mobile banking. Your account and personal information could be intercepted with an unsecured Wi-Fi network.
- **Review your accounts frequently**
  Review your transactions and report any suspected fraud or other account issues to us immediately.

Everyday Mobile Banking Safety Tips

- Don't store username and passwords on the device
- Don't allow any app to automatically login to your mobile banking account
- Always log out of your mobile banking account
- Encrypt your sensitive information
- Frequently delete text messages received from the credit union
- Don't respond to text messages or emails asking for personal information
- Don't click on links in texts or emails from unfamiliar sources
- Don't allow downloads from unknown sources

For More Information

www.lsfcu.net/security

If You Suspect a Compromise

If you suspect, notice or experience any suspicious activity with Lafayette Schools CU online banking, mobile banking or your debit/credit card, you should contact us immediately.

Debit Card & Online/Mobile Banking Fraud
1-866-989-2800

Credit Card Fraud (FIS Card Services)
1-800-600-5249

You can also visit any Lafayette Schools CU branch during normal business hours to report suspicious account activity, discuss any security-related events, and receive a copy of our Electronic Fund Transfers Agreement.

R05/2014

LAFAYETTE SCHOOLS CREDIT UNION

Smart Financial Solutions.

337-989-2800 | 866-989-2800 | lsfcu.net