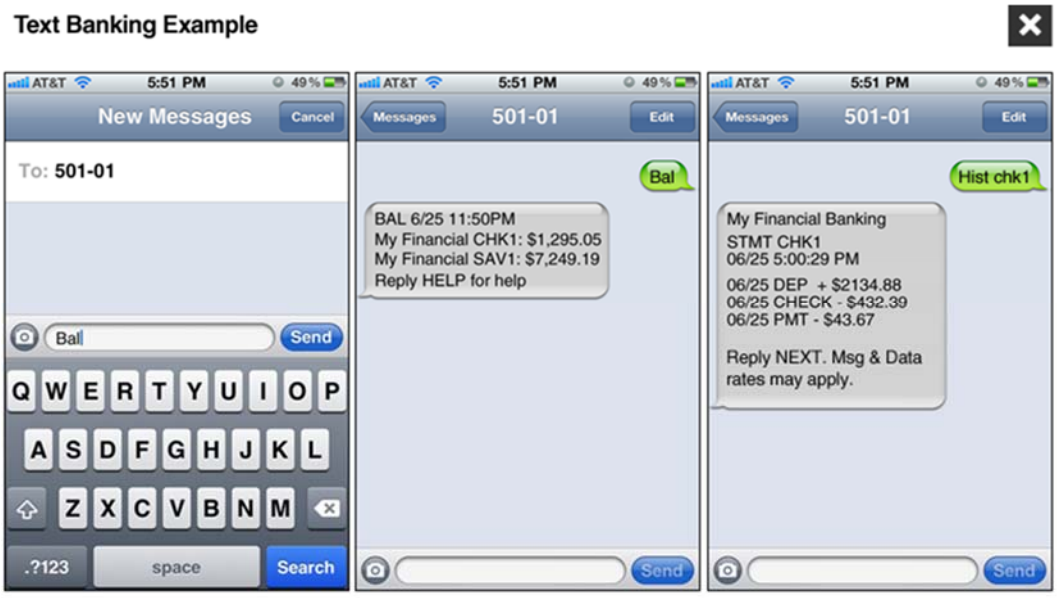
Customer Education to Combat Scams and Fraud

How you can protect your identity and accounts:

- Do not click suspicious links or open unexpected attachments.
- Do not provide account info to links in emails or texts.
- Do not provide account info over the phone to live or automated systems other than FFSL phone banking at
    - Toll Free - 888.378.2067
    - Lorain - 440.282.2961.
    - Huron - 419.433.9629
    - Sandusky - 419.624.9663
    - Port Clinton - 419.734.7477
    - Always verify the identity of the person on the phone by calling back a known number.
- Do not use unknown or unsafe devices to access your account.
    - This includes cell phones, tablets or computers.
- Use only phones, tablets and computers with the latest software and security patches.
    - Use auto-update for all programs to receive the latest security patches.
        - Windows XP is no longer updated by Microsoft. Consider upgrading.
    - Use anti-virus software and keep it updated.
    - Keep your browser updated.
    - *See instructions page below to turn on auto update and to activate Microsoft Security Essentials.*
- Even with these recommendations, you the consumer must remain vigilant and suspicious of requests for information in order to protect yourself. Be very careful and report all suspicious activity to FFSL immediately.
- Report fraud immediately. Call us at 800 – 589 - 8850

List of FFSL methods of contact:

- FFSL will never text you directly. You may receive texts if requested from mobile banking regarding Balance inquiry or alerts you set up.



- The texts will generally come from this number only - 48179
    - The texts will never compel you to call a number.
- FFSL will never ask you to enter or give account information to an automated phone system outside of telephone banking mentioned previously.
    - You should always be suspicious of requests for personal banking information.
- FFSL does not have any robo or automated calling or texting outside of the alerts.
- FFSL may email you from your online banking product, but the email will most likely not include links to websites. When in doubt call us. They may include phone numbers to call which will most likely be an 800 number or a published number.
    - The email will never ask you to reply.
    - The email will never have an attachment.
    - The email will not include active links.
        - It may include an advisement to go to the website for information, but not a link.
    - These emails will come from customersupport@firstfedlorain.com
- FFSL may call you individually from approved numbers listed below, but if you were not expecting the call, you should always call back a known number which is listed below.

List of approved phone numbers.

Calls from FFSL will originate from these numbers, and you should call these numbers to verify identity.

Main Office: (440) 282-6188

Homewood Office: (440) 277-5809

Huron Office: (419) 433-2437

Port Clinton Office: (419) 734-5568

Amherst Office: (440) 984-4009

Avon Office: (440) 934-3340

Sandusky Office: (419) 626-5576

Instructions Page

This only provides instructions on Windows updates on Windows computers. Your computer will have other programs that you need to set up for automatic updates such as: Adobe, Java, and other browsers such as: Google Chrome or Mozilla. You will also need to investigate your tablet and phone to learn how to protect it.

How to turn on Windows automatic update:

http://windows.microsoft.com/en-us/windows/turn-automatic-updating-on-off#turn-automatic-updating-on-off=windows-7

From Microsoft:

To have Windows install important updates as they become available, turn on automatic updating. Important updates provide significant benefits, such as improved security and reliability. You can also set Windows to automatically install recommended updates, which can address non-critical problems and help enhance your computing experience. Optional updates and Microsoft updates are not downloaded or installed automatically.

For more information about automatic updating and installing Windows updates, see **Understanding Windows automatic updating** and **Install Windows updates in Windows 7**.

To learn more about the types of updates that Microsoft publishes, go to the **Microsoft updates terminology** article on the Microsoft Help and Support website.

1. Open Windows Update by clicking the **Start** button  . In the search box, type **Update**, and then, in the list of results, click **Windows Update**.

2. In the left pane, click **Change settings**.

3. Under **Important updates**, choose the option that you want.

4. Under **Recommended updates**, select the **Give me recommended updates the same way I receive important updates** check box, and then click **OK**. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.

You can also choose if you want to allow anyone to install updates by selecting the **Allow all users to install updates on this computer** check box. This applies only to updates and software that are installed manually; automatic updates will be installed regardless of the user.

How to turn on Microsoft Security Essentials (Anti-virus)

http://windows.microsoft.com/en-us/windows/getting-started-with-security-essentials

From Microsoft:

There's not much to do. Microsoft Security Essentials works in the background to protect your PC. It checks for updates automatically a few times a day and doesn't slow your PC down while it works.

Simple color-coding, simple actions

You can keep track of how your PC is doing by looking at the Microsoft Security Essentials icon in the notification area at the far right of the taskbar. Green means everything is okay, yellow means that your PC is potentially unprotected, and red means that your computer is at risk.

When you see yellow or red, click the icon and you'll be able to see the details and take actions. Usually the best thing to do is to choose **Clean computer** so that the threat can be removed.

If you want to delete threats automatically whenever they are identified, open Microsoft Security Essentials, click the **Settings** tab and then choose **Default actions**.

Scanning right now

Open Microsoft Security Essentials and you'll be on the **Home** tab. You can select a **Quick** scan or a **Full** scan (and then click **Scan now**).

The quick scan will look for viruses in all the places they are most likely to hide. It's a good choice when you're just checking on the health of your PC.

But if something makes you think your PC is infected with a virus or spyware, we recommend a full scan. Your computer will be a little slower while it is running, but the full scan looks everywhere for possible problems.

Scheduling scans

By default, Microsoft Security Essentials runs a scan of your PC once a week when you're probably asleep (2:00 am on Sunday).

If you want to adjust this, open Microsoft Security Essentials and click the **Settings** tab. Under **Scheduled scan**, you'll be able to change the day and time as well as the type of scan.

Scanning more than just your hard drive

It may be useful to scan external drives and USB drives since they can get infected too.

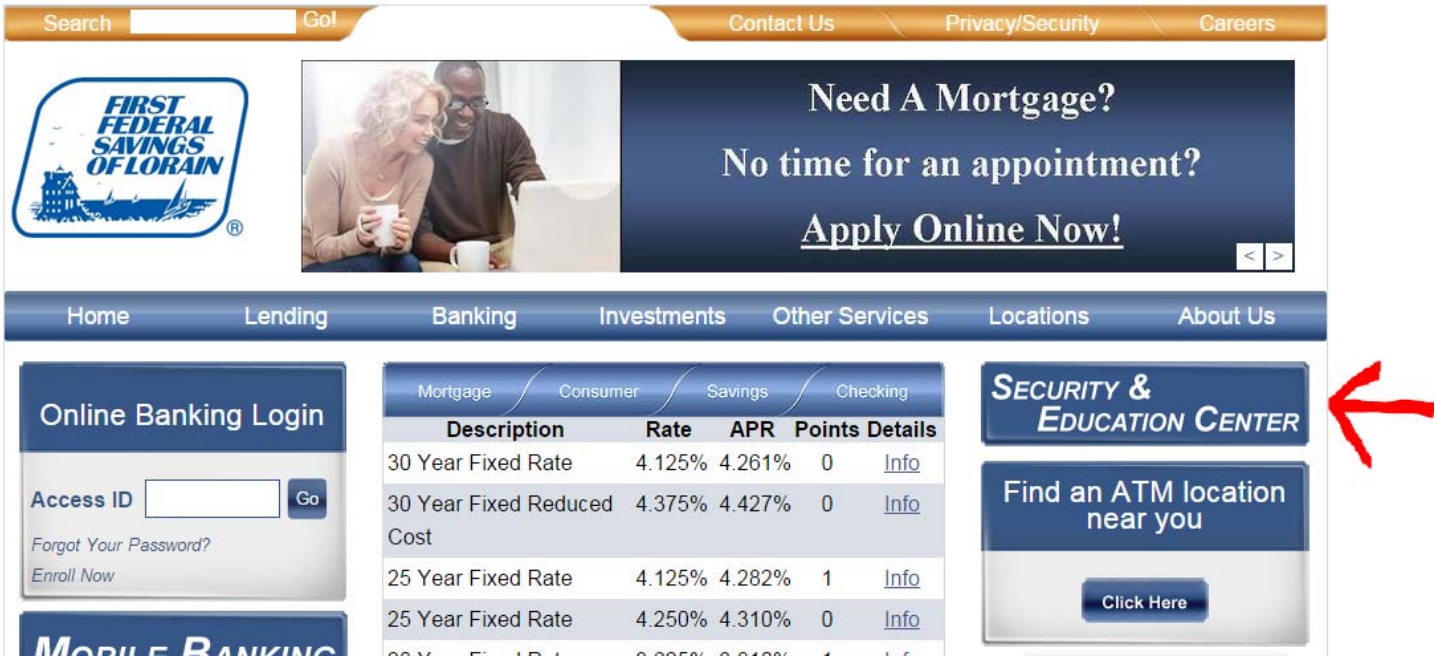
Open Microsoft Security Essentials and click the **Settings** tab. Go to **Advanced** and click the option to **Scan removable drives**. Whenever scans run, your removable drives will also be scanned (if they're attached to your PC). If you want to run a scan right away, go back to the **Home** tab and click **Scan now**.

Bill Pay in Online Banking

- Online banking requires you to use an email account.
  - Protect access to this account at all times because it is used for communication from online banking.
- If you elect to use online banking, you can then register for bill pay.
- Once you register for bill pay, payees can be established.
  - Recipients receive the money in one of two ways depending on the recipient's capability:
    - Paper check
      - These are cut and sent in advance of the scheduled day.
    - Electronic ACH
      - These are transferred on the scheduled day.
      - These funds are immediately transferred on that day.
- What are the risks of using bill pay?
  - If you do not protect your computer or device in the manner described above, a hacker could take over your machine.
  - After taking over your machine, they could watch you login into online banking.
  - After learning your online banking credentials, they could add themselves as a payee in online banking and pay money out of your account into theirs.
- Ways to protect yourself
  - Secure your device as described previously.
  - Monitor your emails diligently for notifications of changes to your online account and payees.
  - Log into your account regularly and check your balances, activities, and payees.

Learn More About Security

On our website, click the Security and Education Center button.

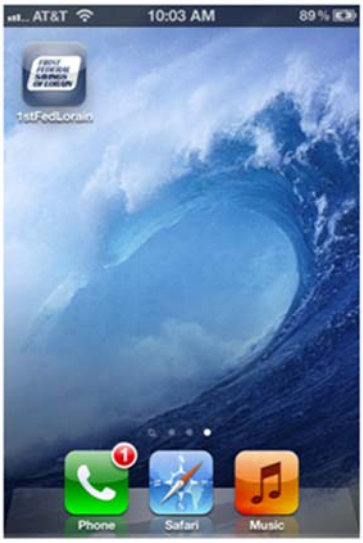


Or go here http://www.firstfedlorain.com/security__education_center/

Mobile App Examples

Android

iPhone



Start up screen

Log in screen

Mobile Browser Banking Site Example

Mobile Browser Examples