First Federal Bank of Ohio

Customer Education for Fraud
Web, Phone & Mobile

TABLE OF CONTENTS

Combat Scams and Fraud

Protect Your Identity and Accounts

- Do not click suspicious links or open unexpected attachments or texts. Be aware of Phishing emails and SMiShing texts.
- Do not provide account info to links in emails or texts.
- Do not provide account information over the phone to live or automated systems other than FFBO Anytime Access phone banking at 877.772.2237.
    - 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. See Securing Your Device.
    - **Windows XP and Windows Vista (as of 4/11/2017) are no longer updated by Microsoft. Consider upgrading to Windows 10.**
        - https://www.microsoft.com/en-us/windows/windows-10-specifications?OCID=win10_null_vanity_win10specs
    - Use anti-virus software and keep it updated. See Securing Your Device.
    - Keep your browser updated. See Securing Your Device.
- ***We are providing these instructions as a courtesy only. We cannot and will not provide any support beyond providing these written instructions. Do not call for technical support.***
- 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 FFBO immediately.
- Report fraud immediately. Call us:
    - Main Office: 419.468.1518
    - Toll Free: 888.888.4314.
- To report a lost or stolen VISA or MASTERCARD credit card, call 800.325.3678
- To report a lost or stolen VISA DEBIT or ATM card, call:
    - During business hours: 419.468.1518 or contact your local First Federal Branch
    - After hours only: 800.472.3272

Approved FFBO Methods of Contact

Website: https://firstfederalbankofohio.com/

Support: 419.468.1518

Text

- **FFBO will never text you directly.**

Debit card texts

- You may receive texts from Fiserv regarding debit card charge verification.
  - See SMiShing info below.
  - You have to opt-in for the texts.
  - For support call 419.468.1518
  - Customers may request alert samples from the bank. Text Alert Samples.

Online Banking alert texts

- You may receive texts from online banking (Fiserv) regarding alerts you set up.
  - The alerts are similar to the email alerts and are configured in the same area.
  - The text will come from alerts@firstfederalbankofohio.bank in the form of text message. See SMiShing info below.
  - The texts will never compel you to call a number or to supply additional personal information.
  - Customers may request email alert samples from the bank. Text Alert Samples.

Credit Card Text from FIS

- If you have a credit card from FFBO, you may receive text alerts from FIS in the case of suspicious transactions.
  - The texts may come from 800.369.4887.
  - The texts will ask you if you intended a specific transaction.
  - First asks about transaction and amount, merchant reply yes or no.
  - Customers may request email alert samples from the bank. Text Alert Samples.

Automated Calls

- **FFBO 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.

Debit Card Calls

- You should always be suspicious of requests for personal banking information.
- FFBO does not have any robo/automated calling or texting other than debit card charge approval from Fiserv.
    - That number is 877-253-8964

Direct Human Call

- **FFBO may call you individually from approved numbers, 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 FFBO will originate from these numbers, and you should call these numbers to verify identity.
        - Main Office and Galion Branch: 419.468.1518
        - Mt. Gilead: 419.946.8010
        - Cardington: 419.864.5255
        - W. Fourth St. Mansfield: 419.529.4687
        - Lexington Ave. Mansfield: 419.756.5494
        - Shelby: 419.347.8066
        - Sandusky: 419.626.8900
        - Tiffin Loan Office: 419.443.8300
    - If you filled out a mortgage application, you may receive a call from a loan officer from a number listed above.
    - You may receive calls from Fiserv about debit card fraud.
        - That number is 877-253-8964

Credit Card Calls - FIS

- **FFBO has automated calling related to credit card transactions which originate from FIS.**
- The calls originate from 800.369.4887 and are from live operators.
- The operator will identify as calling on behalf of First Federal bank of Ohio.

Email

- **FFBO generally will not email you directly except in the following circumstances. Email will usually not include links to websites.**
    - They may include phone numbers to call, which will be 419.468.1518.

Online Banking Email Alerts

- Email alerts about your accounts will usually come from alerts@firstfederalbankofohio.bank
    - The email will never ask you to reply.
    - The email will never have an attachment.
    - Some alerts are configurable - Online Banking Email Alert Configuration in figures below
    - For support call 419.468.1518
    - Customers may request email alert samples from the bank. Email Samples.

eStatement Email

- **You must opt-in to receive eStatement notices. Once enrolled you will receive eStatement availability notices by email.**
    - The email will come from nondeliverable@firstfederalbankofohio.bank
    - For support call 419.468.1518
    - Does not contain attachments or links except for link to adobe.
    - Customers may request email alert samples from the bank. Email Samples.

Credit Card Email – FIS

- If you have a credit card from FFBO, you may receive email alerts from FIS in the case of suspicious transactions.
- The emails will come from FraudServiceCenter@financialinstitutionname.com.
- The emails will ask you if your transactions are authorized and ask you to click one of two links.
- Customers may request email samples from the bank. Email Samples.

Mortgage Application Email

- **If you filled out a mortgage application, you will possibly receive an email from one of our loan officers.**
  - The email from address will look like this jsdaoe@firstfederalbankofohio.com and be sent to the email you provided in your application.
  - When in doubt call the bank office you use. See numbers below.
  - Customers may request email alert samples from the bank. Email Samples.

Beware of Phishing Emails

What is Phishing?

Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels.

Typically, a victim receives a message that appears to have been sent by a known contact or organization. An attachment or links in the message may install malware on the user's device or direct them to a malicious website set up to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details.

Phishing is popular with cybercriminals, as it is far easier to trick someone into clicking a malicious link in a seemingly legitimate email than trying to break through a computer's defenses. Phishing campaigns are often built around the year's major events, holidays and anniversaries, or take advantage of breaking news stories, both true and fictitious.

To make phishing messages look like they are genuinely from a well-known company, they include logos and other identifying information taken directly from that company's website. The malicious links within the body of the message are designed to make it appear that they go to the spoofed organization. The use of subdomains and misspelled URLs (typosquatting) are common tricks, as is homograph spoofing -- URLs created using different logical characters to read exactly like a trusted domain. Some phishing scams use JavaScript to place a picture of a legitimate URL over a browser's address bar. The URL revealed by hovering over an embedded link can also be changed by using JavaScript. From TechTarget

10 Tips to Prevent Phishing Attacks

1: Learn to Identify Suspected Phishing Emails

There are some qualities that identify an attack through an email:

- It could duplicate the image of a real company.
- The email may copy the name of a company or an actual employee of the company.
- It might include sites that are visually similar to a real business.
- It may promote gifts, or the loss of an existing account.

2: Check the Source of Information from Incoming Mail

Your bank will never ask you to send your passwords or personal information by mail. Never respond to these questions, and if you have the slightest doubt, call your bank directly for clarification.

3: Never Go to Your Bank's Website by Clicking on Links Included in Emails

Do not click on hyperlinks or links attached in the email, as it might direct you to a fraudulent website. Type in the URL directly into your browser or use bookmarks / favorites if you want to go faster.

4: Enhance the Security of Your Computer
Common sense and good judgment are as vital as keeping your computer protected with a good antivirus to block this type of attack. In addition, you should always have the most recent update on your operating system and web browsers. See Below.

5: Enter Your Sensitive Data in Secure Websites Only
In order for a site to be 'safe', it must begin with 'https://' and your browser should show an icon of a closed lock.

6: Periodically Check Your Accounts
It never hurts to check your bank accounts periodically to be aware of any irregularities in your online transactions.

7: Phishing Doesn't Only Pertain to Online Banking
Most phishing attacks are against banks, but attacks can use any popular website to steal personal data such as eBay, Facebook, PayPal, etc.

8: Phishing Knows All Languages
Phishing knows no boundaries, and can reach you in any language. In general, they are poorly written or translated, so this may be another indicator that something is wrong. If you never go to the Spanish website of your bank, why should your statements now be in this language?

9: Have the Slightest Doubt, Do Not Risk It
The best way to prevent phishing is to consistently reject any email or news that asks you to provide confidential data. Delete these emails and call your bank to clarify any doubts.
1-9 From PandaSecurity.com

10: Change Your Passwords Frequently and When in Doubt
Change your passwords regularly – at least 4 times a year. Change it more if you can stand it. If you suspect you have been tricked by a phishing email, immediately change the password and notify your bank.

Beware of SMiShing Texts

What is SMiShing?

SmiShing or SMS phishing is about sending false, fake text messages, claiming the mobile user that they have won a free product or need to enter information or correct an account mistake. Within the fake text message, there is a fake URL link that would lure the individual into clicking the link or a fake phone number. After the user has clicked the link, that is when the hacking starts. The phone number may be to a hacker waiting to steal your info to use at an ATM.

They may request:

- Credit card information
- Account passwords
- Account information
- Other valuable information

Recognize a SMiShing Attempt

There are several indicators of an email or text message scam, including:

- Generic greetings.
    - Instead of using your name, many message scams begin with a general greeting, such as: "Dear [Company Name] customer."

- Incorrect account information.
    - The message will attempt to scare you with a large account balance, a warning that someone has recently updated your account or a prize or special offer that must be claimed quickly.

- A false sense of urgency.
    - The message will attempt to compel you to act by threatening that your account is in jeopardy if you don't update your information as soon as possible, or with a short deadline to claim a prize or special offer.

- Fake links.
    - Links may appear valid, but typically go to fraudulent websites. Always check where a link is going before you click. On a computer, you can do this by hovering your mouse over the link (without clicking it) and looking at the website address in your browser's status bar, which is usually in a bottom corner of the screen. If it appears suspicious, don't click the link. Alternatively, go directly to the company website from your browser, not through any links sent in messages.

What to Do? Tips to Prevent Becoming a Victim

1: Avoid clicking on any UNKNOWN messages with links. Furthermore, think about who sent you the message. Is it a person that you know?

2: Do not reply to text messages that have asked you about any of your personal finances.

3: If you have received any messages in regard to your business assets or the partnerships that you have with them and/or the bank that is associate with them, call the business or businesses to see if it is a legitimate request before responding.

4: Be on the lookout for messages that contain the number "5000" or any number that is not a phone number. This is a strategy where scammers have masked their identity so their location and identity are not traceable.

5: If the text messages (along with the unknown number) urges for a quick reply then that is a clear sign of SmiShing! Don't Respond!

6: Do extensive research before replying to any message. There are plenty websites that allow anyone to run search based on a phone number and see any relatable information about whether or not a number is legit.

7: Never call back a phone number that was associated with the text that concerns you.

8: If the message states "Dear user, congratulations, you have won...." It is a clear sign for SmiShing.

9: Check the time when the unknown message was sent. If the text message was sent at an unusual time, then that is another sign of SmiShing.

10: Make sure to be aware and informed of your bank apps policy. It is important to acknowledge there is a policy that protects your money along with other personal information that is associated with the bank account.

11: Send the fraudulent message to the bank and wireless carrier.

12: Delete the fraudulent message.

Secure Your Windows Devices

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.

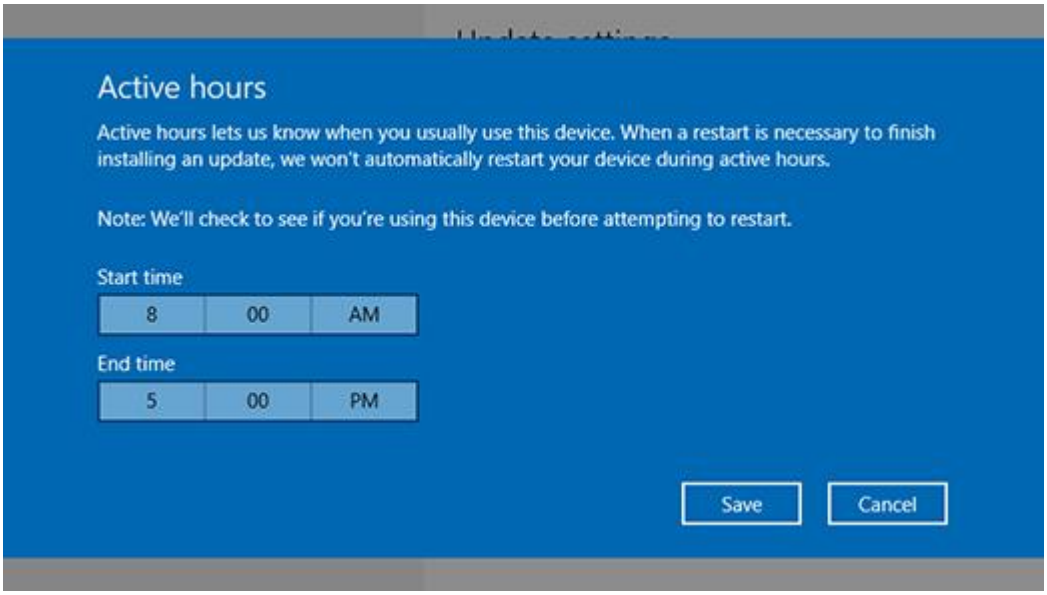
****** We are providing these instructions as a courtesy only. We cannot and will not provide any support beyond providing these written instructions. Do not call for technical support.***

Windows 7 and Windows XP are no longer supported by Microsoft. Update your operating system to Windows 10.

How to Turn on Windows Automatic Update for Windows 10:

https://support.microsoft.com/en-us/help/17154/windows-10-keep-your-pc-up-to-date

1. Select the **Start** button, then select **Settings** > **Update & security** > **Windows Update**, and then select **Change active hours**.



2. Choose the start time and end time for active hours, and then select **Save**.

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 will 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**.

How to Turn on Windows Defender for Windows 10

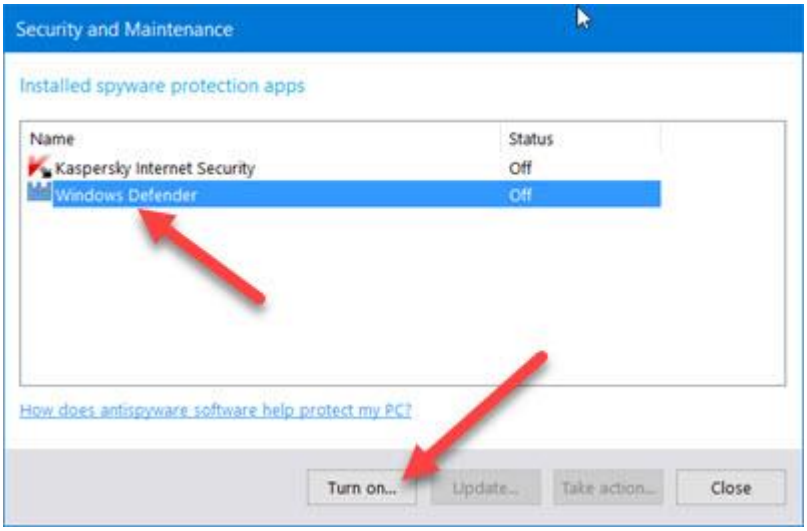
To start Windows Defender, you have to open the Control panel and Windows Defender Settings and click on *Turn On*, and ensure that the following are enabled and set to On position:

1. Real-time protection
2. Cloud-based protection.

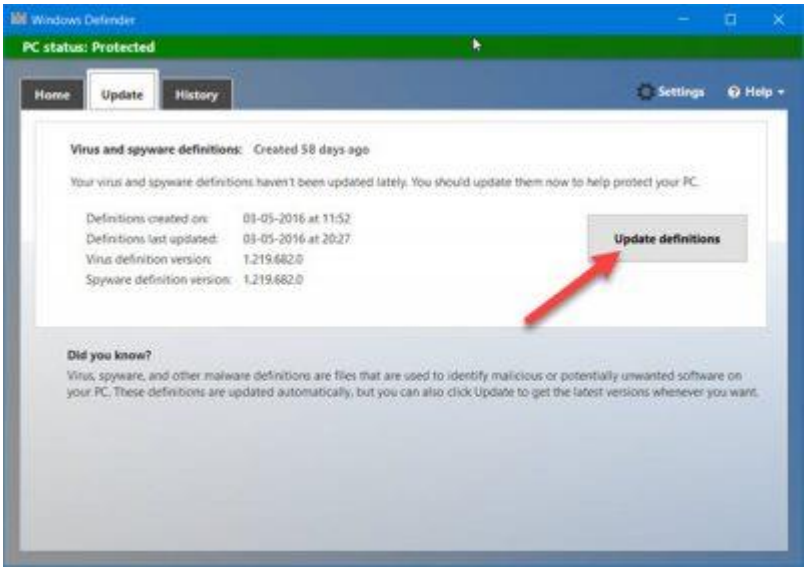
When there is no security software protecting your computer, you will see notifications like these appear.

Clicking on it will show you the installed security apps on your system. If you miss this notification, you can see it in the Notification & Action Center.

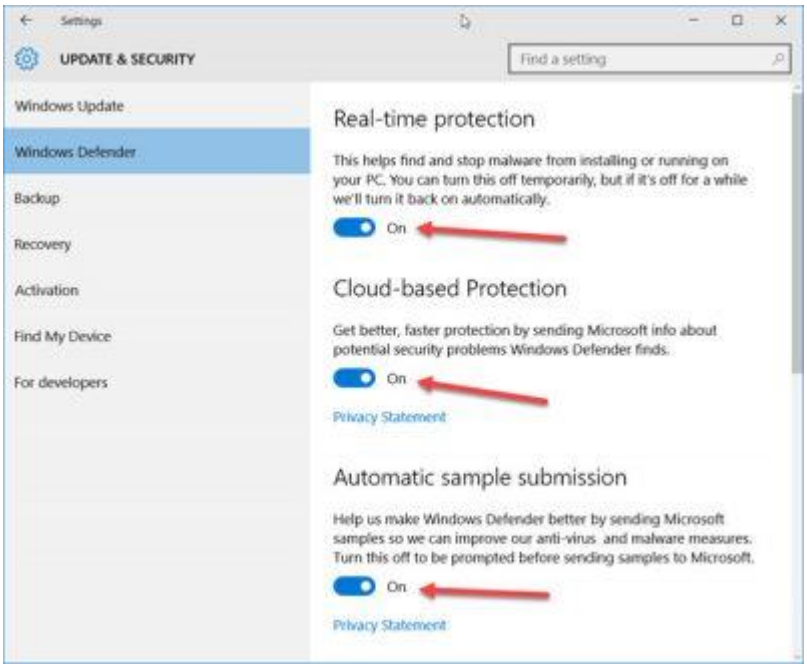
Clicking on it too will show you the installed security apps on your computer, as follows.



Select **Windows Defender** and then click on the *Turn on* button. Windows Defender will start. The first think you want to do when this happens, is to update your definitions.



Clicking on the Settings link in the top right corner will open the following panel. You can also access it via Settings > Update & security > Windows Defender.



Once here, ensure that *Real-time protection* and *Cloud-based protection* is set to On. You may also set *Automatic sample submission* to the On position. You may then configure Windows Defender according to your needs.

Windows Firewall – Turn It On

Always, always turn on Windows Firewall.

Windows 10

To turn Windows Firewall on or off, select the **Start** button, open **Windows Defender Security Center** > **Firewall & network protection**, choose a network profile, and then under **Windows Firewall**, turn it on or off.

Backup Your Device

You need to plan ahead so that you can recover from attacks. Many attacks like ransomware ruin, corrupt, or lock the data on your computer. You can combat that by regularly taking backups of your machine. Use an external hard drive and/or a secure cloud service to do perform your backups. Many of these solutions require very little technical skill to use, but can save your important data.

Home Router

Take the time to understand your home router and use its firewall or security capabilities.

More from Microsoft

Please go to this page and read more tips guidance from Microsoft.

https://support.microsoft.com/en-us/help/17228/windows-protect-my-pc-from-viruses

https://support.microsoft.com/en-us/help/4013550/windows-protect-your-pc-from-ransomware

Additional Resource

https://staysafeonline.org/stay-safe-online/online-safety-basics/

Secure Your Android Device

From TechRepublic http://www.techrepublic.com/blog/10-things/10-security-measures-you-should-take-with-your-android-device/

1: Do use strong passwords
...For everything mobile. Every. Single. Thing. From your lockscreen to your email, to your app logins. No password should be simple to remember or enter. You've heard this countless times, but it always, always, always bears repeating. First, not having a lockscreen password shouldn't even be considered an option. Second, never use a simple password for this first line of defense. Ever. Make this password (PIN or pattern) as complicated as you can handle. The more complicated your password, the harder it will be for others to get to your data.

2: Do use two-factor authentication on everything possible
Google, Facebook, Amazon: They all offer two-factor authentication. Employing this on each service should not be an option. When these accounts get hacked, bad things happen. You can lose money, you can lose friends, you can lose information. Two-factor authentication can go a long way toward preventing this from happening—and it's not difficult to do. You'll definitely want to make use of the Google Authenticator or Authy to dole out the six-digit keys to get you into your accounts.

3: Do encrypt your device
Yes, your device performance will take a slight hit, but the added security is worth it. Once you've encrypted the device, you'll add an extra required password (during boot) that can't be circumvented. If you purchase a newer Android device (one that shipped with Marshmallow), you're already enjoying full device encryption. To find out if your device is encrypted, go to Settings | Security and look for the Encryption section. If it is listed as Encrypted, you're good to go.

4: Do use a password manager
You shouldn't allow any apps to save your password for you, unless the app is designed specifically for saving passwords. The last thing you want to do is have all your passwords cached on your mobile device. If you lose it (or it gets stolen), all those passwords are there for the taking. Instead of saving the passwords, use a solid password manager (like 1Password). Yes, this will be a bit of an inconvenience, but the added security will be well worth it.

5: Don't skip the updates
There's a reason why apps update, and it's not just for features. Apps update to fix security issues as well. If you don't bother to update those apps, you may leave yourself open to security flaws that could lead to terrible, horrible, no good, very bad... issues. You should always update your apps. The longer you wait, the longer your device stands vulnerable.

6: Do lock your apps

There are apps in the Google Play Store that allow you to secure other apps with passwords. This means you can choose which apps you want to password protect. Once protected, those apps can be opened only after entering the required password. No password, no entry. One of my favorite apps for this purpose is AppLock. It's reliable, easy to use, free, and does the job without adding so many bells and whistles as to complicate the process.

7: Do manage your app permissions

Thanks to Android Marshmallow, managing app permissions is finally in the hands of the end user. This means you can remove permission for an app to, say, access the device mic or camera. For example, you don't want Facebook to be able to use your location. You can now disable that particular feature from the app. To do this, go to Settings | Apps and then tap the gear icon and tap App Permissions. The system is straightforward and does a great job of empowering the user. Just make sure you don't disable permissions for system apps (which are hidden, by default, in the Permissions Manager window).

8: Don't use open Wi-Fi networks

If you're at a coffee shop and its wireless network is not password protected, don't use it—especially if you'll be transmitting sensitive information. If you find yourself faced with an open wireless situation, use your carrier network instead. If you have no choice, use one of the many VPN services available (such as TunnelBear VPN). When using an open network through a VPN connection your data will at least be encrypted and a bit more challenging to abscond with.

9: Don't install apps from a third party

You may be tempted to install that really cool sounding Android app from a third party. Don't. You never know whether that app might contain a dangerous piece of malware that could walk away with your sensitive information. Limit yourself to only installing from the Google Play Store. Even then, read the reviews of the app in question before installing. A few minutes of your time to check into an app (prior to installation) will be well worth the effort.

10: Do add your device with the Device Manager

Google has this handy tool called the Android Device Manager. Once your device is added, you can track it if it's lost—or even remotely wipe it, should you fear that your sensitive data could become compromised. To enable this feature, go to Settings | Google | Security and then tap to switch on both Remotely Locate This Device and Allow Remote Lock And Erase. You should do this immediately with your device. If you don't, and you lose your device, the Device Manager will do you no good.

Bonus tip: Do use the guest account feature

When handing over your device to another user (for whatever reason), make use of the guest account feature. If you pull down the notification shade (on Marshmallow, you must do this twice), you'll see a small icon representing your user account. Tap that icon and you can then add a guest user. Once added, when you hand that device over, tap the user icon to switch to the guest account. Making use of this system means the guest user can't access your data (unless they know your security password/PIN/pattern).

Secure Your iOS Device

From COMPUTERWORLD http://www.computerworld.com/article/3047179/apple-ios/14-privacy-and-security-settings-every-ios-user-should-use.html

1: Alphanumeric passcodes
You probably already use a 4-digit passcode, but you can improve that with a 6-digit or alphanumeric code. You change this in Settings>Touch ID & Passcode, select Change Passcode and then tap the small Passcode Options dialog you'll encounter. Alphanumeric codes are the toughest to decipher, so use one. You should also do yourself a favor and set up Touch ID.

2: Erase data
At the bottom of the Settings>Touch ID & Passcode screen you'll find the Erase Data toggle. Set this to green and all data on your iPhone will be erased after 10 failed passcode attempts.

3: Two-factor authentication
One of your most powerful protections, two-factor authentication means that when you enter your Apple ID and password for the first time on a new device, Apple will ask you to verify your identity with a six-digit verification code using one of your other devices. Manage this on your Apple ID account page.

4: Find My iPhone
Don't be a loser – enable Apple's Find My iPhone (Settings>iCloud>Find My iPhone) on all your devices. You should also enable Send Last Location in order that your iOS device will share the last place it was before battery life expires.

5: Location protection
Your iPhone automatically gather your favorite locations. This can be useful, but you can turn this feature off in Settings>Privacy>Location Services>System Services and then Frequent Locations, which you must turn off. You can erase data that may already have been gathered by tapping the Clear History button. You can also control which of Apple's system services are tracking your location by taking a look at Settings>Privacy>Location Services>System Services. Here you can review those Apple apps that use your data and disable the ones you don't use, but don't disable Find My iPhone.

6: More location
Many apps request access to that data even when you're not using them. You can review what permissions you've given to which apps in Settings>Privacy>Location Services, where you can assign location permission access to each app. Limiting access to this data may limit what some apps can do, but the trade-off is privacy – you can always change the setting when you want to use an app, and are you sure you wanted to share location data with an app you used just once?

7: Who gets your data?
Many apps seem demand access to personal data such as email, contacts of calendar information. Do you know why? Apps will ask for permission to use this information, but you can change and review how much access you provide to third party apps in Settings>Privacy and select which apps you trust enough to use this data.

8: Hard payments
Is it really too time-consuming to manually approve every purchase you might make on your iPhone? Protect yourself by choosing Always Require when a payment dialog appears.

9: Delete iMessages
Do you want your iMessages to be read by anyone who might break into your iPhone? No? Open Settings>Messages and in the Keep Messages section set 30-days, the shortest period Apple allows.

10: Lock screen
Previews of messages, notifications and emails can appear on your lock screen, meaning anyone in possession of your device can monitor these communications, even if they can't get into your phone. Change this in Settings>Notifications>Messages and Mail. Maximize privacy by disabling Show Previews so your communications won't appear on the lock screen.

11: Passcode free?
You can leave Today, Notifications View, Siri, Reply with Message, Wallet visible and (to a point) accessible on your lockscreen, but you can disable this for each of these in Settings>Touch ID & Passcode.

12: Safari privacy
Ads networks want your data. Not only do they want this to sell you stuff, but they also try to make dollars selling demographic information about you to advertisers. Control what you share in Settings>Privacy>Advertising and enable the Limit Ad Tracking toggle. You should then tap the Reset Advertising Identifier tool to anonymize yourself. And avoid using Google services.

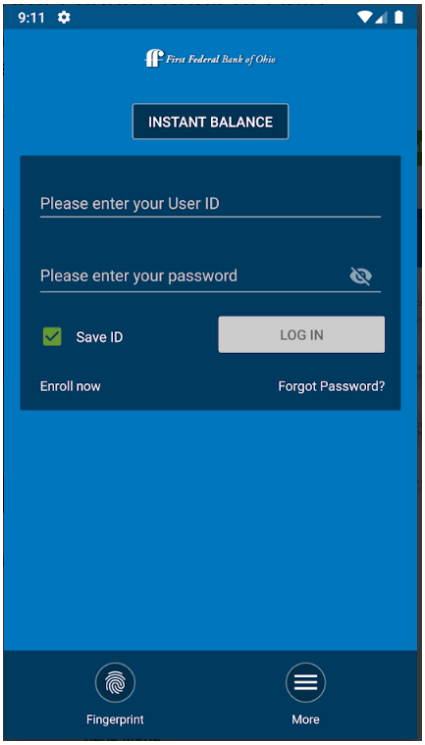
13: Use DuckDuckGo
Change your search engine to DuckDuckGo in Settings>Safari>Search Engine, because the search engine doesn't collect information about you.

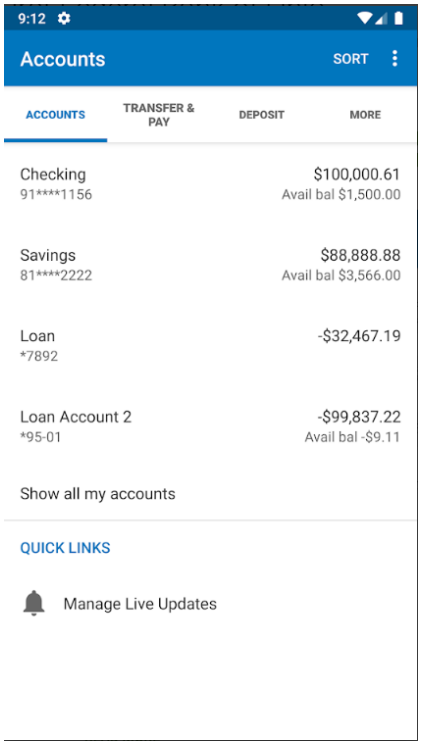
14: Auto-lock
Lower the auto-lock time to 30-seconds in Settings>General>Auto-Lock.

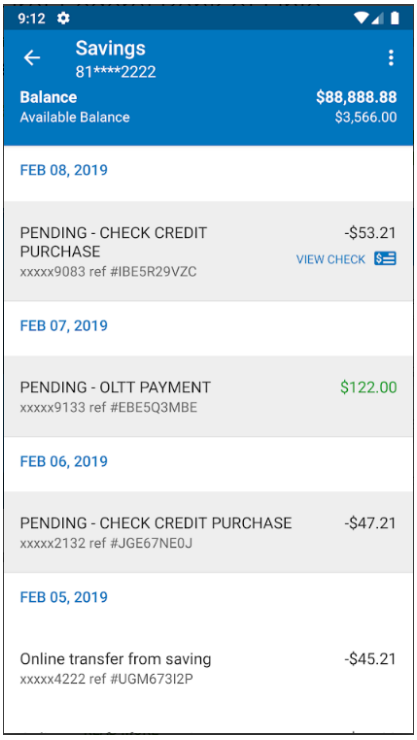
Mobile App Downloads

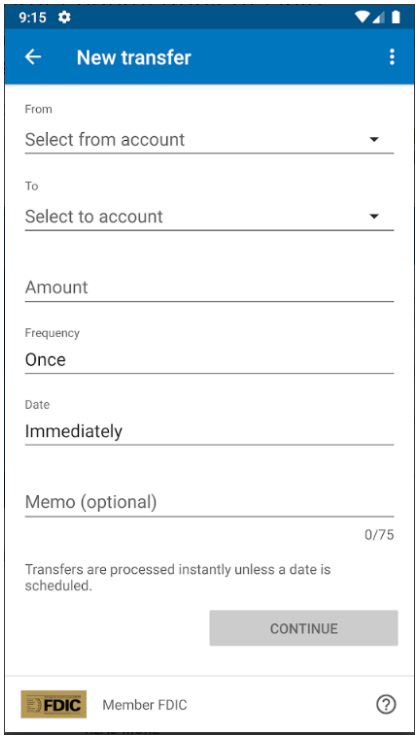
Android

You need to be an active online banking user to use Mobile Banking.
https://play.google.com/store/apps/details?id=com.firstfederalbankohio.mobile&hl=en_US



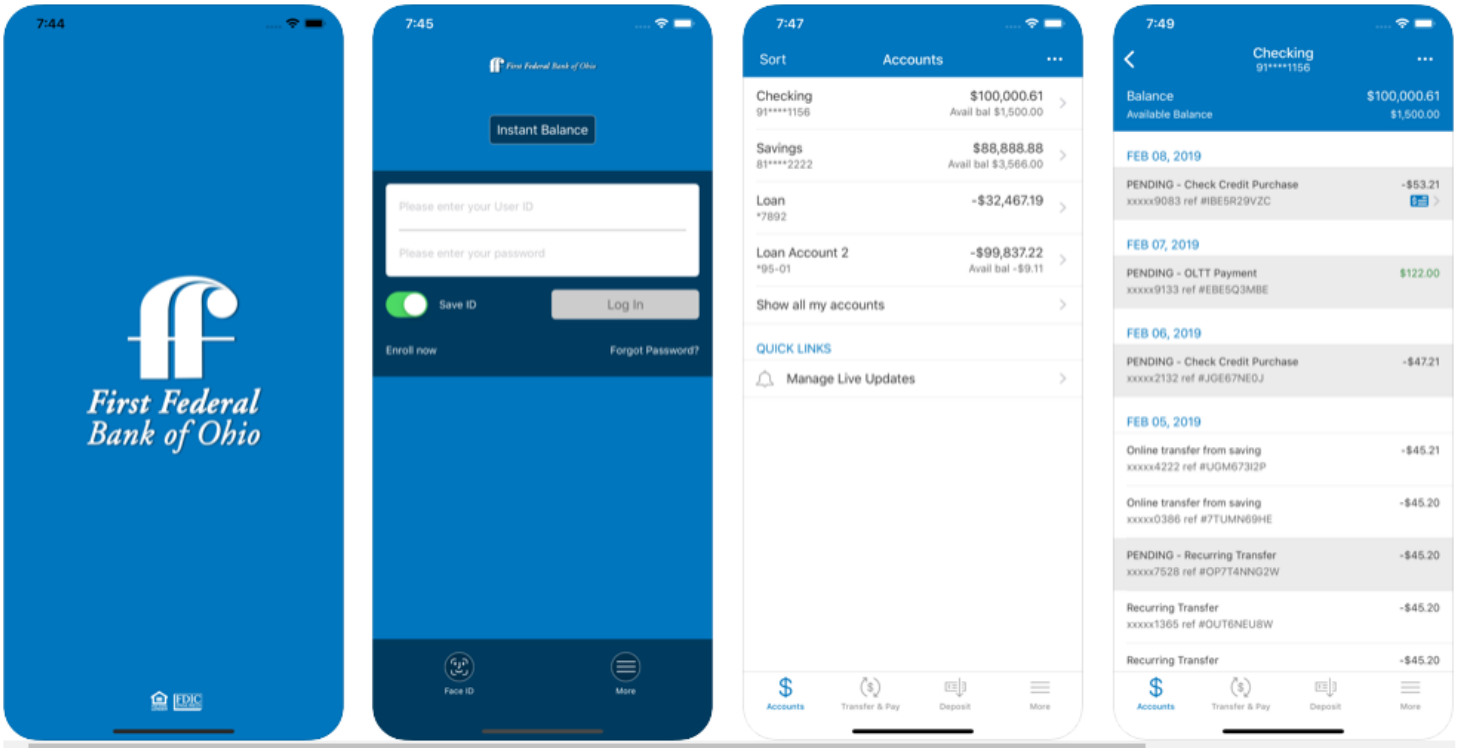


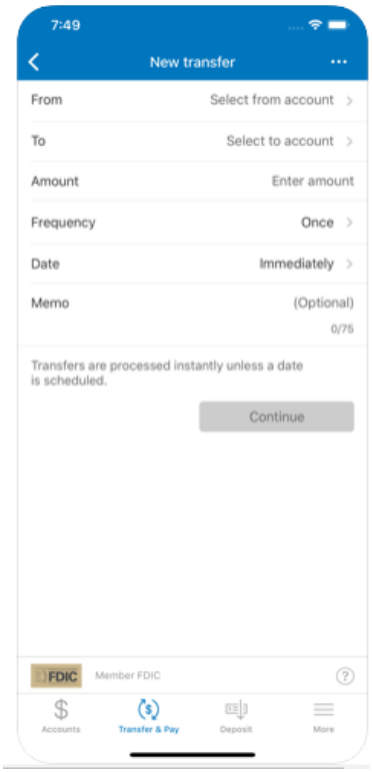




ITunes

You need to be an active online banking user to use Mobile Banking.
https://apps.apple.com/us/app/first-federal-bank-of-ohio/id1482416256





Online Banking Information

Overview of Security

The Internet Banking login process includes several layers of security. This security is intended to prevent unauthorized access to your account, validate your identity, protect your account information from fraudulent use, and prevent the theft of your identity.

Security Data

The following security information, which you set up during an initial login session, is used to protect your Online Internet Banking sessions:

- Initial login askes for
  - Account #
  - SSN# - You will not use this after enrolling
  - Pin#
  - DOB
  - Email
  - Question from your credit report
- If all the info is correct according to your account, you will automatically have online banking access.
- To log in, you will then use
  - Username, password, or fingerprint on your mobile phone
- On new devices or if you do not select remember my device you will have further authentication to perform
  - Three security questions with answers you chose
  - no codes, no photos

Security Question/Challenge

A security challenge occurs when your financial institution's online banking software does not recognize the computer from which you are attempting to log in. The purpose of the security challenge is to prevent unauthorized people from accessing your account information.

The challenge requires you to prove your identity by correctly answering one or more of the challenge questions you selected when you set up the authentication security data.

Online Banking Screenshot

Customers can request samples of online banking screens from the bank. Online Banking and Bill Pay Samples.

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 funds are immediately transferred on the scheduled day.
- For Support call the bank.

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

- Log into your account regularly and check your balances, activities, and payees.
- Secure your device as described previously.
- Monitor your emails diligently for notifications of changes to your online account and payees.

Bill Pay Screen Samples

Customer can request samples of bill pay screens from the bank. Bill pay samples.

Business Online Banking Customer Education

Communication

Text

- **Functions the same as the personal online banking.** Text information

Phone Calls

- **All calls will come from the bank from the numbers listed previously.** Call information

Email

- **Emails function the same as the personal product.** Email information

Other Capabilities

- You may be approved to do remote deposit capture and wires. If so, the bank will issue you an rsa token that you must protect and keep secure.

Security Guidance

Business Online has enhanced electronic transaction capabilities. It is extremely important that you heed all the guidance in this document. Businesses should also consider additional security measures.

Business Security Measures

- Use a hardware firewall to protect your business network.
    - Block unnecessary traffic, services, and websites.
- Use Windows domain security features.
    - User accounts
    - Passwords with complexity requirements, expiration, attempt limits.
- Limit employee access to only what is necessary.
- Patch, Patch, Patch all devices.
- Consider purchasing commercial grade antivirus and keep it updated.
- Scan your network internally and externally for vulnerabilities regularly and remediate the vulnerabilities.
- Back up and encrypt your important data regularly.
- Use encryption when transmitting data.
- Encrypt mobile devices.
- Limit the use of removable storage.
- Train and educate yourself and your staff.
    - Phishing
    - Smishing
    - Securing Devices

What is Dual Authorization?

Dual Authorization is an important control in which a business can require two authorized employees to complete separate actions in order for an electronic transaction to be completed. This provides protection against insider malicious activity or from one compromised machine or user account. If your business can support this control, we recommend using it.

What else can you do?

- Keep your transaction limits as low as possible.
- Monitor accounts and transactions regularly and carefully.
- Use complex passwords, protect passwords for Business Online, and change them frequently.