

What's the Difference between ACH & Wire Transfer?



In today's digital economy, many people prefer to receive employment compensation through direct deposit. They also find it more convenient to pay bills and send money electronically rather than using checks. This form of electronic fund transfer is called an

automated clearing house (ACH) transaction. Another form of electronic fund transfer is the wire transfer. Although the end result is the same, there are differences between the two, mainly in the cost and time of delivery.

ACH Transactions

ACH transactions are next day or future-dated transactions. For example, the bill payments you schedule in your online banking account are transferred by your bank in a group or a batch, along with all their other customer's scheduled payments, usually at the end of the business day. The batch is sent to the clearing house as a single transaction to be processed, as opposed to a direct bank-to-bank transaction. Banks also receive their ACH transactions in a batch as well. This process is secure, simplifies the transfer of funds, and because it's completely automated, each individual transaction does not need individual attention. Unlike a wire transfer, ACH transactions are not immediate and may take a full business day or more to be processed.

Wire Transfers

A wire transfer, on the other hand, is a direct bank-to-bank transaction that allows you to move money from your account directly into the account of someone else. Wire transfers are fast and secure; and can take place in real time.

Wire Transfer Services

Western Union and MoneyGram are other types of wire transfer services. They do not necessarily require any form of identification and can be conducted anonymously. But this is where fraud can take place because people are sometimes scammed into transferring money under false pretenses to an individual they don't know well, if at all. For example, scam emails requesting money claim that a friend or relative of yours is stuck in a foreign country with no money are commonplace. They come from hackers who have gained access to the email account of your friend or relative.

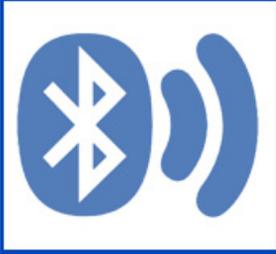
Transferring funds, either by ACH or wire, is generally safe when using a financial institution. However, if your computer has become infected with malicious software (malware), cybercriminals can steal usernames and passwords and defeat common methods of user authentication employed by financial institutions. You can protect yourself from malware by adopting safe online practices and keeping your computers and network secure. Learn how to secure them in other articles found on the Security Center page of our website.

A *true* financial partner makes your dreams possible.

As a true financial partner, Trustmark has helped individuals and families with home financing solutions for generations. When you are ready to take that step, we will be here to provide mortgage options for any situation or stage in life. Discover why we are more than just another bank. Call or visit us today to learn more. **People you trust. Advice that works.**



Protect Your Bluetooth Device from Hackers



Did you know a cybercriminal can gain access to your phone without touching it? When Bluetooth is activated on your phone, a malicious individual can connect to it, run a code and gain full control of it, ultimately viewing keys and passwords. Nearly every connected

device out there has Bluetooth capability. Bluetooth allows our gadgets to effortlessly connect and communicate with others, and hackers can take advantage of Bluetooth technology. Additionally, a Bluetooth attack can allow access to computers, speakers, car entertainment systems and other Internet of Things (IoT) devices.

In most cases, malware depends on people clicking on a link they shouldn't have. With Bluetooth, all a hacker needs to spread malware is for their victim's device to have Bluetooth enabled. It can spread without the victim doing anything and the attack is invisible.

Fortunately, remote hacking poses a relatively small risk today, thanks to firmware updates deployed by technology vendors. Even so, mobile security is an ongoing concern especially when considering the amount of personal and financial information stored on most devices.

Decrease your chances of becoming a victim by following these tips:

- Disable your device's "discoverable" setting to protect it from unsolicited spam messages sent to phones with Bluetooth turned on.
- Require Bluetooth devices to authenticate -- via a PIN -- and use encryption while transferring information from one device to another.
- Never blindly hit the "accept" button when the device receives a file, since it might be a virus or Trojan code.
- Never "jailbreak" or "root" a mobile device. Malware can infiltrate if the user has manipulated the device's factory-installed operating system.
- Disable automatic connections to open Wi-Fi and only connect to trusted networks.
- Educate users about security. Create security policies covering the acceptable use of any device used to store or access confidential information.
- Regularly download and install security updates. Device manufacturers will release updates to address threats and correct weaknesses.

Attacks against improperly secured Bluetooth implementations can provide attackers with unauthorized access to sensitive information and unauthorized use of Bluetooth devices and other systems or networks to which the devices are connected. Learn more at Bluetooth.com or see your cellphone manufacturer's website for more advice.

myTrustmark

More freedom. More features. More control.



Mobile Deposit

Deposit checks on-the-go from your mobile device.



Pay People-Popmoney®

Send money to your friends and family no matter where they bank.



ManageMyMoney

Create budgets and view activity on all of your accounts in one place.



External Transfer

Easily transfer money between your accounts.

Enroll today at trustmark.com



Member FDIC

*Same-day processing available until 9 p.m. CST weekdays; funds may not be available for up to 5 business days.

Popmoney is a registered trademark of Fiserv, Inc., or its affiliates. Terms and conditions apply.



Trustmark National Bank
Offices in Alabama, Florida, Mississippi, Tennessee & Texas