Paying a bill, depositing a check or conducting any other financial transaction used to require a trip to the bank or post office. Now technology makes it possible to bank and pay bills without leaving your home or office.

Online banking is safe and offers many advantages over branch banking. But that doesn't mean you should let your guard down. While financial institutions take many measures to keep out intruders, you, too, should take precautions to protect your personal data and accounts. Once you know what to watch out for and what tools are available to enhance your security, you can enjoy the benefits of online banking while minimizing the risk.

What is online banking?

Online banking, also known as internet banking, lets you access your accounts and make the most common types of transactions using a computer and internet connection. Virtually all financial institutions, including banks, credit unions, lenders and investment companies, offer online banking. There are even banks that offer *only* online accounts.

You can set up your current checking/savings accounts for online banking, or you can open a new account online. To open a new account, first choose the institution you want to do business with. (*Bankrate.com* allows you to compare checking and savings accounts available in your area.) Once you choose a bank (or credit union), you can go to its website and apply for an account. Typically, you will find online applications under "personal banking." You can open an individual account, or a joint account with another person. The application will ask you to:

- Provide your personal information, including name, address, phone number, Social Security Number, and ID, such as a driver's license number. For joint accounts, both applicants must provide this information.
- Fund your account with an initial deposit. Most banks require at least a "minimum deposit" to start, but you can add as much money as you want. You can do this by providing the account number for an existing bank account or a credit card. You may be able to save your application and send a check in the mail if you can wait several days for the account to be opened.
- The bank will send you documents to sign and mail back.

Just because you apply for your account online does not mean you will have access to online banking. As with existing accounts, you may need to visit your financial institution's website and register for website access by providing your account details and email address, and choosing a username and password. During this process, you may be asked for your mobile phone number to enable "two-factor authentication," an extra measure of protection against intruders (the bank sends a code to your device, which you must enter before gaining access to your online account). In addition, you may be asked to answer several secret questions, which you would be asked if you ever forgot your username.

Generally, you can access checking and savings, credit card, investment and loan accounts online.

Once your online account access is established, you can log in to the system by entering your user identification (which might be your email address, or a username you created) and your password. If you have more than one account at a single institution, such as a checking and a savings account, you can click on the account you want to access.

Depending on the institution and the types of accounts you have, while you are logged in you may be able to:

- check your current balance
- view account activity (deposits, withdrawals and payments)
- read and download your statements
- search for particular transactions (by date, amount, check number or payee name)
- view canceled checks
- transfer money between accounts
- pay bills (you enter payee information and choose when the bills will be paid)
- view account terms (such as interest rates, fees and due dates)
- set and manage alerts, request a stop-payment, or order checks
- contact customer service by instant chat or secure email

> ***TIP:*** *Confused? Most financial institutions offer a "test drive" for online banking in the form of a video or virtual tour of the site. Watch and learn!*

To end your online banking session, sign off (or log out) and close your browser. If you walk away during a session, most financial services websites will log you out automatically after a period of inactivity. Log back in to continue.

Online banking benefits

Convenience is the main reason people bank online. With direct deposits and electronic bill payments, online banking customers can avoid going to a branch or mailbox. And, account information is available 24/7—no more waiting for the monthly statement.

Lower cost is another benefit of online banking. Not only can you avoid the cost of postage to mail bills, you reduce the number of checks you must buy. "E-accounts"—accounts that require that all or most deposits and other transactions be made electronically—often are free or low-cost, even if you don't keep a minimum balance.

Online banking risks

While there are many advantages to banking online, there may also be some disadvantages. These include:

- temporarily losing access to your account, either because you don't have access to a computer, the internet connection is interrupted, or the institution's system is temporarily "down"
- missing a payment because you don't notice the email that alerts you to your online bills
- "phishing" and other scams that try to convince you to provide your login information
- data breaches (the theft or unintentional release of information held in an institution's database)
- failure to protect your usernames and passwords, which could allow a stranger to access your account
- a lost or stolen debit card

> Most bank accounts come with a "debit card" bearing the Visa or MasterCard logo so that, in addition to making transactions at the automated teller machine (ATM), you can also make purchases at stores and online and even get "cash back" on purchases (at the grocery store, for example). When making purchases, you can use your debit card with your PIN (personal identification number) or by signing your name. (If your bank issues an ATM-only card, it can't be used for making purchases—only for transactions at the automated teller machine.)

Safer online banking

Banks and other financial institutions work hard to ensure a safe, problem-free online banking experience. But there are things you can do to increase the likelihood that your personal information will remain private and your accounts will stay secure.

- Make sure that any institution you do business with is legitimate. (A fancy website doesn't prove anything.) Start by reading about the bank in the site's "About Us" section, and then try to verify the information. For example, call the phone number provided. Also, do an online search to find any posts about the institution, including consumer complaints.
- Bookmark your bank's site instead of typing in its web address (URL), as you could make a typo and end up on a "spoof" site—a fake website designed to look like a legitimate business's site and trick you into entering your login information. Before you set the bookmark, double-check to be sure you've typed the URL correctly.
- Verify that the bank is insured. The FDIC name and logo indicate that the bank's customers will be reimbursed for losses on their deposits up to $250,000 if the bank fails. But don't just trust the presence of a logo on a website. Confirm that the institution is insured by visiting the FDIC's website (*www.fdic.gov*), where you can search by the bank's name, city, state or ZIP code. While a bank that is not FDIC-insured may be legitimate, its customers may not be

covered in case of a loss. (Investments, such as individual stocks and bonds, mutual funds, annuities, etc., including those held in an individual retirement account (IRA), are not FDIC-insured.) (The NCUA provides similar insurance for credit unions. Check if a credit union is covered at https://www.mycreditunion.gov/share-insurance.)

- Research the institution's policies. For example, what does its privacy policy say about how it will use your personal information? Does it offer a "zero liability" guarantee for any unauthorized transactions? Will it reimburse any late fees if your bill payment isn't sent as scheduled?
- Create a strong password for your account. The longer and more random the password, the harder it is for someone to figure out, especially if you use a combination of capital and lowercase letters, numbers and symbols. Don't make a password out of a pet's name, birthdate or other personal information.
- Keep your ID/username and password private. Don't share it with anyone and don't leave it where someone could find it. Change your password immediately if you think it has been compromised. Don't allow your browser to "Remember my password" or "Remember me on this computer" for financial accounts.
- Log off the banking website when you are done with your session or if you have to step away from the computer, and close the browser window after signing off. On shared computers, clear your "cached" activity by clicking on the "Tools" menu (in most browsers) and selecting "Clear Recent History" or something similar. (The words may be slightly different depending on the browser you use.)
- Password-protect your home wireless network so that strangers can't access your wireless internet account and possibly capture the data you send and receive. If the router was supplied by your internet service provider, contact the company for instructions on how to do this. If you own the router, check the manual or the manufacturer's website.

> Phishing emails are fraudulent messages that try to get you to reveal sensitive information by making you believe you are communicating with a legitimate business. Often, these messages include a link to a copycat (spoof) website, which is designed to look authentic and lure you into revealing your personal information. Remember, your bank will never contact you and ask for your Social Security number or password via email or phone.

- Use a firewall, which is a virtual barrier between your computer and the internet. Your computer's operating system (OS) may have a built-in firewall; make sure it's turned on. Update your antivirus and antispyware software to guard against new malware as it appears.
- Avoid online banking when using public or unencrypted wireless networks (Wi-Fi). If you must use public Wi-Fi, take precautions. Look for the closed padlock or unbroken key in the browser frame and an "s" after "http" (https://) in the web address, which indicates an SSL (Secure Sockets Layer) connection.
- Don't send sensitive information via email, chat or instant messaging (IM).
- Know how much time it takes your bank to get a payment to your creditors after receiving your online bill payment request. Some payments, typically to larger creditors, are made electronically and may reach their destination within a day or two of your request. Payments to smaller creditors, such as your dentist, may take a week or more because the bank sends an actual check to the recipient. Leave plenty of time for payments to reach your creditors before the due date.
- Monitor your account activity regularly—even daily. In most cases, you must report unauthorized account activity to the bank within a certain time period, and the longer you wait, the more money you could potentially lose. If you don't report unauthorized transactions within 60 days of when they first appeared on your statement, you may not be reimbursed.
- Check your statements every month, even if you fail to get an email reminder. Place a reminder on your calendar of when to check for a new statement each month.

Assistance and information

If you are already a customer, you can contact the financial institution's customer service department for help with online banking. The following resources may be helpful when considering a new financial institution or to learn more about staying safe online.

Federal Deposit Insurance Corporation (FDIC)
www.fdic.gov / 877-275-3342

Contact the FDIC to confirm that any bank you are considering doing business with is insured.

National Credit Union Administration (NCUA)
www.ncua.gov / 800-755-1030

The NCUA administers the National Credit Union Share Insurance Fund (NCUSIF), which provides deposit insurance for credit unions, much like the FDIC does for banks. Visit the NCUA site or call to find out if the credit union you're considering joining is insured.

OnGuard Online
www.onguardonline.gov

The U.S. federal government and the technology industry provide information and tips to promote online safety and security.

Privacy Rights Clearinghouse
www.privacyrights.org

The non-profit Privacy Rights Clearinghouse offers a library of information, from tips for protecting your privacy online to how to shop safely on the internet.

Consumer Action
www.consumer-action.org

Consumer advice and referral hotline:
https://complaints.consumer-action.org/forms/english-form or 415-777-9635
Chinese, English and Spanish spoken

Consumer Action created the Digital Dollar series with funding from Visa Inc.

Visit Visa's financial education program, Practical Money Skills, at: ***https://www.practicalmoneyskills.com***

Rev.3/20

Your Digital Dollars

Banking online safely

Protect your identity and accounts while banking by computer

Financial education from *Consumer Action* and *Visa Inc.*