Share financial data with care

What you need to know about how FinTech apps work
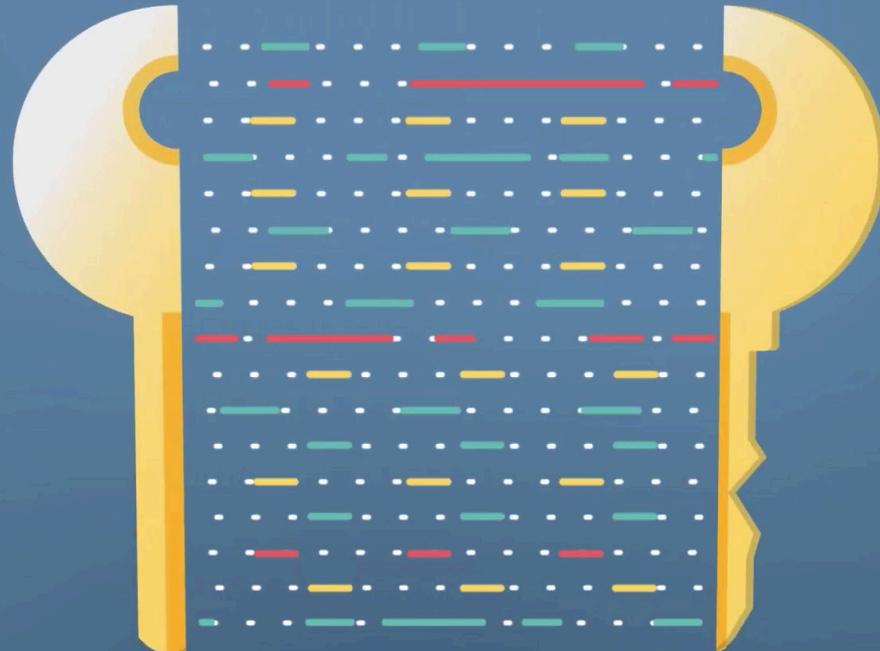
Financial technology—FinTech—makes it possible to accomplish all sorts of financial tasks quickly and easily from a computer, smartphone or tablet. From paying a friend to updating your budget, these tools can save you time and money, and even help you achieve your financial goals.

But before you put FinTech to work for you, it's important to understand how these apps and tools work so that you can get the most out of them while also protecting your personal and account information.

Types of FinTech tools

FinTech refers to any technology that is used to digitize, streamline or enhance financial services. For consumers, this generally means mobile apps, computer software and online (website) platforms.

There are FinTech tools for viewing and managing your financial accounts, sending and receiving money, paying bills, tracking and analyzing your spending, creating and updating a budget, working toward financial goals, paying off debt, saving and investing, planning for retirement, getting a loan, receiving reminders and alerts—and even more.

Some tools are developed specifically for use by an institution's customers and account holders. For example, a lender may offer potential borrowers a way to apply for a loan and, once they have the loan, to manage it (view their balance, make a payment, set a reminder, etc.) via the lender's app. Another example is the IRS app that allows tax filers to check their tax return and refund status.

Many apps and tools are standalone (not created by or for a specific institution). For example, there are apps that enable users with an account at virtually any financial institution to

transfer funds to just about anyone else, regardless of where they do their banking. Another example is an app that rounds up the cost of your daily purchases and transfers the "spare change" to your credit card and loan accounts to help you pay down your debts faster.

Many consumers use a combination of FinTech tools—for example, the apps and online platforms provided by their banks and credit card issuers that enable them to manage their accounts, along with separate tools for budgeting, transferring money, tracking their investments, and so on.

How FinTech tools work

To accomplish the various tasks they are created to do, FinTech tools access users' accounts. For example, a money transfer app would need access to the account from which the funds are to be pulled.

Some apps require access to multiple accounts in order to pull together data from different sources into one spot (your "dashboard").

For example, a budgeting app that tracks income and expenditures might need access to your checking account (to gather information about account deposits, checks written, and ATM/debit card transactions), your credit card accounts (to gather information about card transactions), your PayPal account (for transactions made on that platform), and various bills.

The benefit of gathering data from your various financial accounts is the ability to assess, monitor and manage your finances quickly and easily, in one spot.

When you download a FinTech app or sign up for an account, the tool typically will request your financial institution account login credentials.

Often, you are presented with a login screen that looks very much like a page on your bank's website, even though you are actually providing your username and password to the app (to store for future use) or an intermediary working with the app. Once the company has your ac-

count login information, it may log in to your account, via an automated process, at any time to gather any data it wants (called "screen scraping")—your name, address and other personally identifying information, account numbers, transactions, balances, credit scores, etc.
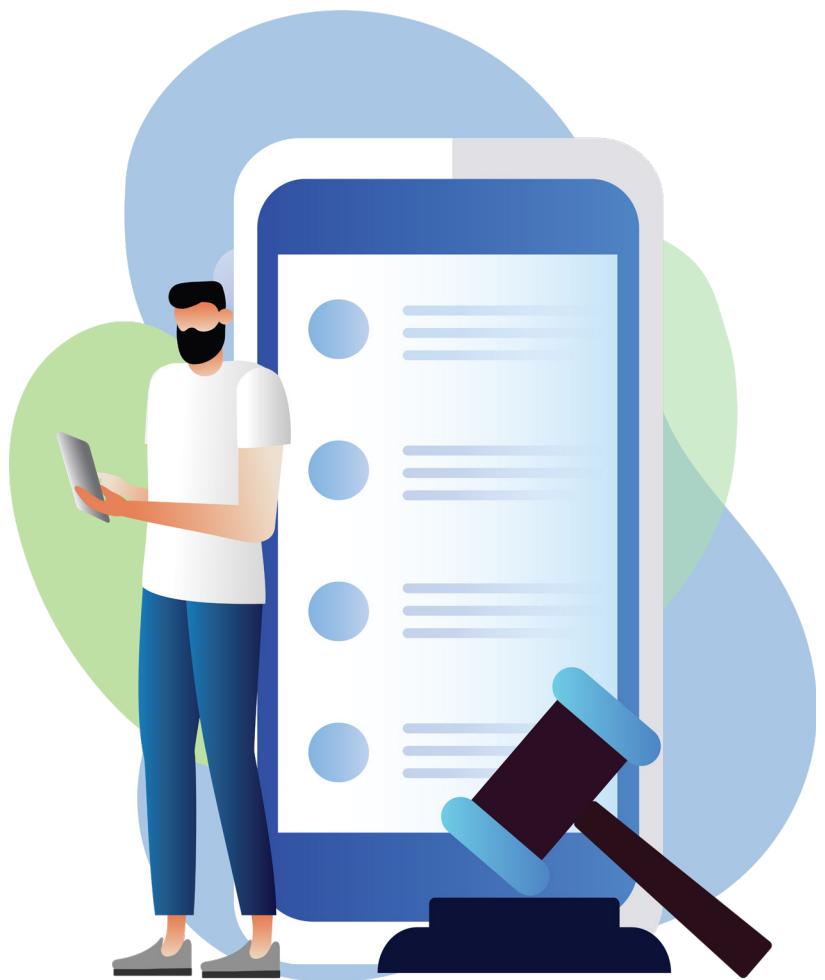
Some apps use an intermediary system that patches your login credentials directly through to your bank, without storing it themselves. This provides an added measure of safety, and can offer greater control over what data the app can collect.

Typically, FinTech tools can store, share and sell the data they collect about you. This is how many "free" apps make money. Sometimes the third-party intermediaries that receive your data are middlemen that help the apps work (for example, enable an app and a bank account to "talk" to each other). Sometimes they are marketing companies that use the data to promote products and services.

Data privacy and security

Reputable FinTech developers take measures to protect users' accounts and data from outsiders. One way they do this is to limit what the tool can do with account access. For example, one popular budgeting app is designed as "read-only," which means the tool (or an outsider who has hacked it) can't initiate a transaction (such as a transfer from your account). Another way is to encrypt user data so that, even if it's exposed, it isn't readable to outsiders.

But intruders are not the only threat to FinTech users' privacy and security. Once the app or tool has your login credentials, it may have unlimited access to your data, for an unlimited time, to be used for unlimited purposes.

For example, depending on its privacy policy—which may be many pages long and difficult to understand—the company might be allowed to gather data beyond what is needed to deliver the intended services, store your data indefinitely, and sell it to any number of third parties for marketing or other purposes.

There also is always the possibility of a data breach—the intentional or unintentional exposure of confidential information. Security breaches and hacking have become common in recent years. The more places your information is stored, the greater the risk of exposure.

Financial institutions have been taking steps to give their FinTech-using customers more control over data shared with third parties. For example, a number of major banks have created dashboards where customers can see which apps are accessing which data, limit access to a particular account or particular information, or even rescind a tool's access entirely.

App developers are also being asked to design their apps so that they don't store users' login credentials. Instead they access an anonymous unique code, or "token," from a trusted third party that completes the "handshake" between the app and the financial institution.

And there are steps that you, as a FinTech consumer, can take to reduce potential risks. These include vetting FinTech tools before using them, limiting the data they can access (when possible), and changing your passwords, as a way to cut off access, when you no longer use the tool.

For more about the specific steps you can take to protect your data, read Consumer Action's companion guide, **Share financial data with care: Privacy and security when using FinTech apps** (*https://consumer-action.org/english/articles/privacy_fintech_apps*).

Visit our **Share financial data with care** webpage (*http://bit.ly/fintech-privacy*) to view a short video and find more information about how to control and protect your financial information when using apps that require access to your bank and other financial services accounts.