Kimberly Palmer, On Monday June 13, 2011, 2:29 pm EDT

Last week's security breach at Citibank was just the latest in a string of incidents that have rattled consumers: Sony, Lockheed Martin, and iTunes are also among recent high-profile targets. With such big names falling victim to hackers, is it still safe to bank online?

The answer, according to top security experts, is a qualified "yes." Using the Internet to bank, buy music, or shop is still as safe or safer than visiting brick-and-mortar locations, as long as consumers take precautions and know what to do if they notice any suspicious activity. In fact, the overall trend is a reassuring one: 2010 actually saw fewer records breached than the previous year due to new infrastructure in place, says Julie Conroy McNelley, senior fraud and risk analyst at research firm Aite Group. Today, she adds, "banks have some of the most sophisticated mechanisms in place."

As long as consumers take a few basic steps (explained below) to help protect their information, security experts agree that online banking remains safe. That's a good thing, since it's almost impossible for consumers to avoid sharing personal data online if they want to participate in 21st-century life, from Facebook to online sales to paying bills. Plus, as McNelley adds, many breaches involve databases of card numbers that exist regardless of how cardholders use their accounts.

Much of online security is out of consumers' hands altogether. "It's actually extremely difficult to know how secure any bank's information-handling is," says Geoff Webb, executive at data protection firm Credant Technologies. Banks often don't share much about their security techniques, since they don't want to tip off criminals on how best to attack them. Whether they talk about it or not, financial firms should be encrypting data, segregating credit card information from other types of data, and making web applications as secure as possible. Regular training of employees is also key, he adds.

In addition to doing what they can to protect themselves on their own, consumers can talk to their representatives in Congress to push for bigger changes, Webb says. The government is becoming increasingly involved in driving the security of banks and other organizations, Webb says. In fact, the Commerce Department recently urged online companies to improve their own security, and President Obama proposed new cybersecurity legislation in May.

Here are 10 steps consumers to take to make sure their information is safe:

1. Don't talk to cyber-strangers, and don't click on hyperlinks within emails from strangers. "That's the easiest way to download malware to your computer," says McNelley. Even if an email looks like it's from a company you know, such as your bank, go directly to the bank's website and log in there instead of clicking on the embedded link, and never open attachments from strangers (or even suspicious-looking ones from friends, who may have been hacked themselves). Sometimes hackers will set up fake sites that look like real sites to capture victims' information, a method referred to as phishing.

"A financial institution will never contact you via email asking you to verify your funds, request your username or password, or any other sensitive information," says Stephen Sims, senior instructor at the SANS Institute, which educates security professionals.

2. Treat your smartphone like the computer it is. Downloaded apps can contain malicious codes, warns McNelley. "You have no idea who created that app, and very little code-checking goes on," she says. If you're going to download apps, she suggests avoiding or minimizing the financial transactions you make with the smartphone. "Mobile phones are really tiny computers, but most consumers don't treat them as such or get anti-virus software for their smartphone," she adds.

Meanwhile, be sure antivirus software on laptops and desktops is up to date. "Many compromises are a result of keystroke-logging software that is illicitly installed on a user's system, capturing usernames and passwords," says Sims.

3. Treat social networks like dark street corners. You never know who's lurking among your friends and acquaintances. Hackers have targeted Gmail, Facebook, and LinkedIn, and users of those sites should be especially wary of clicking on embedded links, even those "recommended" by friends. Hackers also send emails that appear to be from social networking sites but are, in fact, fake emails designed to capture personal information. Again, users should avoid clicking on links embedded in emails.

4. Use the Net to your own advantage. If you bank online, you don't have to wait until the end of the month to check your statement. You can log in anytime and make sure nothing is amiss. An errant charge is often one of the first signs of identity theft, so check statements carefully and alert your bank immediately of any problems.

5. Get free help. Many credit card issuers offer free and automatic identify-theft protection to customers. (That's one advantage credit cards have over debit cards.) If you see erroneous charges on your statement, call your credit card company, which should investigate on your behalf. The law requires credit card companies to dispute erroneous charges. For most people, paying a monthly fee for extra monitoring services is unnecessary. (Once a year, consumers can get their credit report free of charge through annualcreditreport.com.)

6. Think of a new word. Consumers are tasked with remembering dozens of passwords for various retailers, banks, and accounts, making it almost impossible to remember them all, especially since they often include mixes of numbers and letters. Keep careful track of your passwords in a secure document, rely on mnemonic devices to boost your memory, or come up with some other clever strategy--but don't stick with simple passwords that are easy for strangers to guess. Also, change your passwords on a regular basis.

7. Never, ever give your Social Security number to anyone online. If a site asks for it during the checkout process, it's probably a scam site.

8. Shred or safely store financial mail. Bank statements, investment documents, and other financial paperwork can give thieves clues about account numbers, Social Security numbers, and other personal information. Destroying documents with a cross-cut shredder works, but you can make it easier on yourself (and the environment) by limiting your paper trail wherever possible. Shifting to online banking and document storage can reduce your chances of falling victim to a dumpster diver.

9. Fight back quickly. If you are hacked, step one is calling your bank, says McNelley. That's because banks have sophisticated systems in place that can immediately begin closely monitoring your account for signs of identity theft. They can also and shut down and replace any accounts if necessary. In fact, banks are often the first to notice something amiss, even before the victim.

As long as consumers report fraud in a timely manner, the law limits their liability to between $50 and $500, says Sims.

10. Trust your gut. "You often hear, after consumers used an ATM with a skimming device, they

had a bad feeling about it. If you do have that feeling, listen to it," says McNelley, and remove yourself from the situation.

Taking these simple steps is like remembering to lock your door at night, or turn on your alarm system. Says McNelley, "Bad guys go for the house that's unprotected. If you take the basic measures, then generally you have less risk about getting compromised."

Kimberly Palmer (@alphaconsumer) is the author of the new book Generation Earn: The Young Professional's Guide to Spending, Investing, and Giving Back.

Source: http://finance.yahoo.com/news/Is-It-Safe-to-Bank-usnews-4209634978.html?x=0