Keeping your Customer Information is one of our most important responsibilities. But beyond the physical, electronic and procedural safeguards that we employ, it is also important that you stay informed about potential threats to your privacy and financial security outside the electronic confines of this secure online banking resource.

First, some good news: You won't be able to use Landmark Community Bank's online banking services unless your Internet browser supports the highest level of encryption. This prevents transactions from being read over the Internet by unauthorized parties. Look below (on the lower frame of your browser) small icon on your screen that looks like a lock or a key whenever you conduct secure transactions online. In any given year, more than 750,000 Americans have their identities stolen, according to the Federal Trade Commission. Criminals use these stolen identities to establish credit, purchase items or borrow money in your name. The bad guys use a number of methods:

Pretext Calling

Congress made this trick a federal crime in 1999.

The Scam: The thief calls, claiming to work for your bank, needing your account number to verify information. Or, the thief may call your bank posing as you, using information stolen from your mailbox or online. With the stolen information, the thief can take over your account, open accounts at other institutions, and move funds out of your account.

Fighting Back: Monitor your regular credit card and bank statements to be sure they arrive safely. Do not give any bank account information over the phone unless you are sure you know the caller. Never give your Social Security Number over the phone unless you know it will be secure.

Internet Broker Fraud

Online Information Brokers are used legitimately for background checks, to track down debtors or to help find lost relatives.

The Scam: Thieves steal credit card or bank statements from your mailbox or trash. Then they use one of these stolen credit card numbers or your bank account data to gain in depth information about you through online information brokers. This information is gained through email, ensuring their secrecy. The only cost is a small fee which they can charge on your stolen card! These new details allow the criminals to order more credit cards, create phony driver's licenses and steal from your bank accounts.

Fighting Back: Do not respond to spam that promises some benefit but requests identifying data. Never give personal information on-line, except to companies you know to be reputable. Change your passwords regularly, and never reveal your bank account password to anyone.

Phishing

Phishing is a high-tech scam that uses spam or pop-up web messages to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

The Scam: Phishers send an email or pop-up message that claims to be from a business or organization that you deal with — for example, your Internet service provider (ISP), eBay or its subsidiary PayPal, your bank, or even a government agency. The message usually says that you need to "update" or "validate" your account information, directing you to a web site that looks legitimate,
but isn't.

Fighting Back: If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address. In any case, don't cut and paste the link in the message.

Dumpster Diving

The low-tech way to obtain information is still the preferred method for many identity thieves.

The Scam: Criminals raid your mailbox or go through your garbage can or a communal dumpster or trash bin to obtain discarded copies of your checks, credit card solicitations, credit card or bank statements, or other records that typically bear your name and personal information.

Fighting Back: Shred credit card solicitations, ATM receipts and other financial documents before discarding. Report lost or stolen checks immediately. Never leave outgoing mail where it can be stolen.

Evil Twins

These are little wireless networks that pretend to offer Wi-Fi connections to the Internet like those available at some coffee shops, hotels and conferences.

The Scam: On a laptop screen, an evil-twin Wi-Fi hotspot can look identical to one of the tens of thousands of legitimate public networks that consumers log on to every day, sometimes even copying the sign-in page. But that's just a front, and fraudsters who set up the connections attempt to capture any passwords or credit card numbers that consumers using the link may type.

Fighting Back: Turn off your Wi-Fi card when using your laptop offline in public. When you are using it, keep up-to-date protection software that automatically checks a Wi-Fi network's digital ID certificate.

Pharming

The primary victims are ISPs (Internet service providers) that are attacked by hackers. The "pharmers" then lay in wait for the ISP customers' passwords and account numbers.

The Scam: Thieves redirect a consumer to an imposter web page (even when the individual types the correct address into his browser) by changing — or "poisoning" — some of the address information ISPs store. From there, they use the same technique as Phishers (above).

Fighting Back: Check with your ISP and ask if they are protected against DNS cache poisoning. Also, the regular encryption tools in your browser will usually spot frauds.

Check your credit

Contact the major credit reporting companies annually to review your file. The three major credit bureaus are Equifax: 800.685.1111, Experian: 888.397.3742 and TransUnion: 800.916.8800. Order from all three, since each one derives its information from different sources.

12 Habits of Check-Fraud-Free Banking Customers

1. Never respond to unsolicited requests for your checking account, Social Security or other financial information.
2. Safeguard checks at home and on your person; never leave them in your car or workplace.
3. Shred unused checks before disposal, even if they are from a closed account.
4. Destroy convenience checks, such as those that allow cash advances on credit cards, before discarding.
5. Never have your Social Security or drivers' license number preprinted on your checks.

6. When mailing checks, use a heavy envelope or wrap checks in paper to conceal them from view.
7. Notify Landmark Community Bank and U.S. Postal Service authorities if newly ordered checks or routine bank statements don't arrive in a timely manner.
8. Know how many checks you ordered; verify your order and the accuracy of the information on your checks.
9. Immediately notify Landmark Community Bank and file a police report if personal checks, or any checks payable to you, are stolen and then close compromised accounts.
10. Check your balance frequently (you can safely do this online here) and promptly review and reconcile checking account statements for accuracy and fraud.
11. Consider shopping elsewhere if a merchant requires your Social Security number to make a purchase.
12. If you use your Social Security number as your driver's license number, order a duplicate license and request an alternative random number from the Tennessee Department of Safety (if Tennessee issues your license).

Source: America's Community Bankers