www.myaffinitybank.com

AFFINITY BANK SECURITY

Back on Track
At Affinity Bank, keeping your money and your personal information safe and secure is our highest priority. In addition to the safety measures we take on our end, there are precautions you can take to protect yourself as well. When it comes to protecting yourself against identify theft and fraud, there is no such thing as being over-prepared.

Tips to Prevent Identity Theft and Fraud
While identity thieves are resourceful, following the simple measures listed below will help ensure that your personal information is kept as safe and secure as possible.

Email Safety

- ***Don't include sensitive information in email -*** A type of email fraud, phishing, occurs when a perpetrator posing as a legitimate trustworthy business attempts to acquire sensitive information like passwords or financial information.
- ***Never click on links within an email -*** It's safer to retype the Web address than to click on it from within the body of the email.
- ***Don't open SPAM or attachments from strangers -*** If you do not know the sender or are not expecting the attachment, delete it.
- ***Be suspicious of emails asking for personal information -*** Forged email purporting to be from your financial institution or favorite online store is a popular trick used by criminals to extract personal information for fraud.

Online Identity Protection

- ***Be selective when providing your email address -*** If you don't know the reputation of a Web site, don't assume you can trust it. ManyWeb sites sell email addresses or may be careless with your personal information. Be wary of providing any information that can be used by others for fraudulent purposes.
- ***Update and strengthen the security of your online passwords -*** The best password is an undetectable one. Never use birth dates, first names, pet names, addresses, phone numbers, or Social Security numbers. Use a combination of letters, numbers and symbols. Be sure to change your passwords regularly.
- ***Use a secure browser and trusted computer for sensitive transactions -*** Only use secureWeb pages when you're conducting transactions online (a Web page is secure if there is a locked padlock in the lower left-hand corner of your browser or within the Security Status Bar depending on your browser).
- ***Log off when you're done using web sites that require a user ID and password -*** Always logout from your online banking session or any other Web site that you've logged into using a user ID and password.
- ***Disconnect and shut down when you're not using your computer -*** When a computer is not in use, it should be shut down or disconnected from the Internet.

Offline Identity Protection

- ***Monitor your postal mail -*** Identity thieves often search through mail looking for credit card or loan offers and mail them in with your information so they can make purchases using your name and credit line. Protect yourself against identity theft by ensuring your mail receiving habits allow little opportunity for mail theft.
- ***Don't give out your personal information freely -*** Treat your personal information like cash every time you are asked for your personal information – whether in a web form, an email, a text, or a phone message – think about whether you can really trust the request.
- ***Check your credit report annually -*** www.annualcreditreport.com or 1.877.322.8228

If you notice any suspicious account activity or experience any customer information security related events please, contact Affinity Bank at 1.866.736.8194 or onlinesupport@myaffinitybank.com.

Member FDIC

EQUAL HOUSING LENDER

www.myaffinitybank.com

FRAUD TACTICS

Different fraud tactics all share the same goal: to obtain your personal, confidential and financial information for fraudulent use. From obtaining your information 'the old fashioned way' via discarded mail, to emails that ask you to verify personal information under the guise of a trusted source — like your financial institution — fraudulent activity comes in many different forms.

Fraud Tactics Include:

Dumpster Diving:	Thieves rummage through trash looking for bills or other paper that includes your personal information.
Malware:	Also known as "malicious software", malware is designed to harm, attack or take unauthorized control over a computer system. Malware includes viruses, worms and Trojans. It's important to know that Malware can include a combination of all three types noted.
Phishing:	A scam that involves the use of replicas of existing Web pages to try to deceive you into entering personal, financial, or password data. Often suspects use urgency or scare tactics, such as threats to close accounts.
Vishing:	Vishing is a type of phishing attack where the attacker uses a local phone number in the fake email as a means of obtaining your sensitive information. The goal is to fool you into believing the email is legitimate by instructing you that responding to the request by phone is safer than responding by email and shows authenticity. The unsuspecting caller is then tricked through an automated phone system to relinquish their sensitive information.
Pharming:	Pharming takes place when you type in a validWeb address and you are illegally redirected to a Web site that is not legitimate. These "fake" Web sites ask for personal information such as credit card numbers, bank account information, Social Security numbers, and other sensitive information.
Trojan:	A Trojan is malicious code that is disguised or hidden within another program that appears to be safe (as in the myth of the Trojan horse).When the program is executed, the Trojan allows attackers to gain unauthorized access to the computer in order to steal information and cause harm. Trojans commonly spread through email attachments and Internet downloads. A common Trojan component is a "keystroke logger" which captures a user's keystrokes in an attempt to capture the user's credentials. It will then send those credentials to the attacker.
Spoofing:	Spoofing is when an attacker masquerades as someone else by providing false data. Phishing has become the most common form of Web page spoofing. Another form of spoofing is URL spoofing. This happens when an attacker exploits bugs in your Web browser in order to display incorrect URLs in your browser location bar. Another form of spoofing is called "man-in-the-middle." This occurs when an attacker compromises the communication between you and another party on the Internet. Many firewalls can be updated or configured to significantly prevent this type of attack.
Spyware:	Spyware: Loaded on to your computer unbeknownst to you, spyware is a type of program that watches what users do and forwards information to someone else. It is most often installed when you download free software on the Internet. Unfortunately, hackers discovered this to be an effective means of sending sensitive information over the Internet. Moreover, they discovered that many free applications that use spyware for marketing purposes could be found on your machine, and attackers often use this existing spyware for their malicious means.