Technology and online banking has secured a permanent spot in today’s marketplace but how can you best secure your finances with technology? Advancing at alarming rates over the past decade, online banking, which had started to popularize in early to mid 2000s, is now surpassing 62 percent usage, according to a 2015 study by Roy Morgan Research. Online banking isn’t exactly new. Its inception from the early 1980s grew with the rise of the internet but in this mobile age, its conveniences and security are unmatched. We have gone from checking balances and viewing statements to paying bills, depositing checks, and even applying for loans all using a smart phone or mobile device. From managing finances and personal data to social media accounts, there can be a lot of sensitive information accessed by our mobile devices but the good news is keeping your finances secured is easier than you think!

What you may not know is that Central Sunbelt’s online banking platform; the Cloud Branch, does not actually store any personal financial data on your device. This not only means the data is always fresh from the cloud servers online, but it is about as easy to secure as your personal photos or address book, and far less at risk if your device, such as laptop or phone, is lost or stolen.

For those who have not yet delved into the online Cloud Branch, you may be surprised to find it runs on the same rails as the internal system used by our teller and Member Services teams at your local branch. Unlike some financial institutions that use multiple third party services and different software companies for their internal transactions, online banking, and mobile services, Central Sunbelt uses one unified online-based system for everything. This means depositing a check on your smart phone through the Cloud Branch is actually the exact same process as your local teller uses at the teller line and every bit as secure.

Much like the Cloud Deposit example, e-statements via Cloud Documents follow the same path and are accessed in the Cloud Branch in a very similar and equally secured process as performed by your local branch staff. The Central Sunbelt online system generates documents, such as your recent statement, and makes them accessible through a live, online login from our internal staff or by you; through a multi-factor authentication that you set up yourself.

In many ways, viewing your Cloud Documents in the Cloud Branch can arguably be a much safer alternative to mailing sensitive data via the mail system.

If you’re looking to try out the Cloud Branch and need a bit of assistance, feel free to stop by your local branch or give our Member Services team a call!
1. Change your passwords often
2. Secure your e-mail and check often
3. Enable remote wipe on your smart phone device in case your phone is lost or stolen
4. Do not auto-save all your passwords to a device (unless your device uses fingerprint authentication for logins)
5. Use pin login or pattern screen locks with a short screen lock time
6. Use App locks to lock certain Apps behind an additional security wall
7. Never access secured data behind an open WiFi connection
8. Use a remote locator and keep your mobile device location turned on to help locate your device if lost
9. Never input your personal or financial account information into a website or email. If in doubt, always go directly to the company’s website. Scammers will take advantage by pretending to be a company and request sensitive information for 'verification' purposes, tricking you into giving your information away directly to the scammers.
10. Never let someone use your device you do not trust

Paper cuts aren’t the only time paper can be harmful. Identity thieves are getting more and more creative with today's scams but some of the most common occurring practices are still happening through social engineering, mail theft, and paper trails containing personal/sensitive data that is neglected and left behind or thrown away. Social engineering is the method of influencing or tricking a victim into giving up sensitive information. Often times, the targets are those who a thief has some pieces of information already collected. Your probability of being subjected to identity theft is directly related to the efforts you take to minimize risk. A single piece of mail may seem harmless, not containing anything too sensitive or valuable, but it could be the missing piece someone needs to access an account or impersonate you. As a rule of thumb, any mail or paper that has any piece of your information should be disposed of in a secured fashion such as a paper shredder. With enough pieces of the right information, the impact and ease of identity theft is compounded. A thief can begin to divert some or all of your mail using a change of address. Upon collecting pieces of your mail, your information becomes compromised and the thief starts to access your accounts leading to uncovering even more data, or begin impersonating you for financial gain.

Thieves can also attempt phishing for information by claiming you are entitled to something free or have money to claim. One example is a piece of mail you may receive pertaining to a class action lawsuit of a popular product or device. This may claim to award some money and only requires filling out a small questionnaire asking sometimes seemingly harmless information. Some have even reported fake class action lawsuit forms that attempt to trick you by asking for your bank account information to be able to draft your earnings directly into your account.

One effective way of minimizing risk is to minimize or eliminate as many paper trails as possible and administer all of your data sensitive services online. Through this method, you can manage and change your passwords regularly and eliminate unwanted sensitive mail from being sent which can be intercepted before it even hits your mailbox. With some modern devices, you can even establish a PIN based entry or fingerprint authentication when signing into online services to provide an extra layer of protection beyond the standard username / password required to use the device.

The best way to eliminate the industry of scammers is to be vigilant and take all possible precautions to keep your information safe.
Whether you are writing a post on your wall or have just recently left a review on a company’s social media site, scammers can impersonate said company and direct a response towards you that seems rather convincing. For example, let’s pretend you leave a review on World’s Best Insurance’s (your insurance company) social media page and are contacted via a message by World’s_Best_Insurance. They may show empathy or helpfulness in accordance with your recent post/review, quickly followed by social engineering tactics to inquire about personal data needed to access your account to help ‘verify’ you and better assist you; such as your username / password, or mailing address and social security number. Pay close attention to the name and if in doubt, contact the company directly for further communication.

Many of us have seen this before and it applies to places other than Facebook. You may receive a message or email stating that your account has been compromised and you need to verify your information or log in and change your password. The reality is your data is actually safe and the link that is provided will go to a site that collects the data you type, however you’ve just compromised your data by giving your login information to the scammer. This scam has been commonly used against wireless companies, financial institutions, cable/media companies, and is trickling over into social media accounts which can provide direct access to your friends and family while impersonating you.

These can generally be easy to avoid if you live by the “If it sounds too good to be true” rule. Scammers will purchase Facebook accounts and change the profile picture, personal information, and even begin posting to impersonate a made up person. Often times you can scroll down to their dated posts and see long gaps of inactivity followed by a recent string of posts that can depict exactly where that Facebook account was purchased. Typically, the scammer will change their home location to somewhere near you and attempt to appear as a refined, trustworthy person of society to build trust. They may friend you out of the blue and allow a good bit of time to elapse before contacting you so they seem recognizable and familiar when you hear from them again down the road. Inevitably they will either attempt to phish little pieces of information from you bit by bit until they have enough to do some damage, or they may offer you a prize reward by using your account to help wire money. In all cases, this never turns out good for anyone.
Fast Cash
HOLIDAY LOAN

Fast Holiday Cash
Fast Approval
Visit your local branch in November for details!

Are you ready for your Holiday Club PAYOUT?
On November 1st, your Holiday Club cash moves into Savings.
Withdraw at any ATM for your stress-free shopping season.

Not a Holiday Club member yet?
Make shopping next year a breeze and enroll by calling 601-649-7181 option 2.

Holiday Closings

COLUMBUS DAY
Monday, October 10

VETERANS’ DAY
Friday, November 11

THANKSGIVING
Thursday, November 24
Friday, November 25
open until 1:00pm

CHRISTMAS
Saturday, December 24
open until 1:00pm
Monday, December 26

NEW YEAR’S
Saturday, December 31
open until 1:00pm
Monday, January 2, 2017

Central Sunbelt introduces new Petal Branch!
1859 Evelyn Gandy Parkway, Ste. 10
Hattiesburg, MS 39401-1069

YOUR VOLUNTEERS
DIRECTORS
Dale Wood, CHAIR
Chris Diabin, VICE-CHAIR
Kaye L. Ray, SECRETARY/TREASURER
Edwin Todd | Joe Hancock
Thomas I. Williams | Robert Dearman

SUPERVISORY COMMITTEE
Jolynda Moorer, CHAIR
Susan McCall | Dusty Holfield

Qualifying required for financing. APR = annual percentage rate.

Central Sunbelt
Federal Credit Union

MAIN OFFICE
1506 Congress Street | Laurel, MS 39440
Fax 601.518.1167

SAWMILL ROAD
734 Sawmill Road | Laurel, MS 39440
Fax 601.425.9955

LINCOLN ROAD
1857 Lincoln Road | Hattiesburg, MS 39402
Fax 601.261.5596

WESTOVER DRIVE
112 S. Westover Dr. | Hattiesburg, MS 39402
Fax 601.264.0474

MCHEMING
1417 Aston Avenue | McComb, MS 39648
Fax 601.684.1953

WAYNESBORO
345 Central Road | Waynesboro, MS 39367
Fax 601.509.1075

PETAL
1859 Evelyn Gandy Parkway, Suite 10
Hattiesburg, MS 39401-1069
Fax: 601.682.0057

HOURS
Hattiesburg, Laurel, & Waynesboro Business Hours:
Monday - Thursday | 8:30 a.m. to 4:30 p.m.
Friday | 8:30 a.m. to 5:30 p.m.
Saturday: Lobby | 9:00 a.m. to 12:30 p.m.
(excluding Congress Street and Waynesboro offices)
Saturday Drive-Thru | 9:00 a.m. to 1:00 p.m.
(excluding Waynesboro office)

McComb Business Hours:
Monday - Thursday | 9:00a.m. to 5:00p.m.
Friday | 9:00a.m. to 5:30 p.m.

Petal Business Hours:
Monday - Friday | 8:00a.m. to 5:30p.m.
Saturday | 9:00a.m. to 1:00 p.m.

Member Service & Loan Services Hours:
Monday - Friday | 9:00a.m. to 5:30p.m.

ATM Services Hours:
Monday - Saturday | 5:00a.m. to 10:00p.m.
Sunday | 6:00a.m. to 9:00p.m.

Teller Plus Hours:
Monday - Friday | 8:00a.m. to 5:30p.m.
Saturday | 9:00a.m. to 1:00 p.m.

IMPORTANT NUMBERS
MEMBER SERVICES
601-649-7181

Option 1: Sunny 24/7 Audio Teller
Option 2: Member Services Department
Option 3: Fraud Department
Option 4: Lending Department
Option 5: Branch Location Information
Option 6: Financial Counseling

www.sunbeltfcu.org

©CUAdvantage.com • 877.799.0784