GHS FEDERAL CREDIT UNION

WINTER 2021

Offices:

211 Patewood Drive
Greenville, SC 29615
Phone: (864) 288-8046
Fax: 288-8489

Hours
Monday–Friday
9:00 a.m. – 5:00 p.m.

Drive-Up
Monday - Friday
8:30 a.m. - 5:00 p.m.

Greenville Memorial Hospital
701 Grove Road
Greenville, SC 29605
Phone: (864) 455-7945
Fax: 455-8880

Hours
Monday - Friday
7:30 a.m. - 4:30 p.m.

On the Web at:

- www.myghsfcu.coop
- **24/7 Visa Credit Card Online Management at** www.eZCardInfo.com

Important Phone No.'s

Lost & Stolen Cards
After Credit Union Hours
ONLY and Weekends:

Visa Credit Cards:
1-800-991-4964

Visa Check Cards:
1-800-472-3272

EZ Card Info Customer Service
1-800-604-0380

Direct Connect 24:
864-288-8524

AMERICA'S CREDIT UNIONS™
Where people are worth more than money.™

OUR INSTITUTION IS RATED 5-STARS BY BAUER
www.bauerfinancial.com
AWARDED DECEMBER 2020

notes of interest

COVID-19 CYBERSECURITY DOS AND DON'TS

DO:

Update – keep your software and operating systems updated on your computer and mobile device. Updates help strengthen your device protection. Make sure that your passwords and authentications are strong and updated often as well.

Use Caution – when sharing your personal information or making any sort of donation to COVID-19 research or charity, use caution before committing. Make sure that you know who you are giving information or financial support to.

Research – when in doubt, dig a little deeper to find out more information about an email, phone call, or anything at all that you come across that you are unsure about. It is better to be safe than sorry!

Raise Awareness – if you come into contact with a cyberscam using COVID-19 as a ploy, let your friends, family, and coworkers know so that they do not fall victim!

DON'T:

Give Out Personal Information – never give out your personal information such as your address, full name, banking information, or SSN through an unsolicited phone call or through an email from an unknown source.

Click Links – If you receive an email from an unknown source, do not click any links in the email as they can contain computer viruses. Many phishing emails have adopted the COVID-19 pandemic as a strategy to send out malware attacks that appear to be offering health information, treatments, vaccines, benefits, and supplies.

Connect to Unsecure Networks – Network connection has been a new challenge while so many of us are working remotely due to COVID-19. Do not connect to public WiFi networks. They are open for public use, and while they may be convenient, they are the perfect place for your information to be exploited. Make sure that the network you are connecting to is secure.

Download Unknown Applications from the Internet – Sometimes it is easy to just click "download" when something pops up on your computer. Check with security professionals before downloading anything from the internet.

2021 Virtual Annual Meeting

To help ensure the safety of members and staff, this year's annual meeting will be held online on **Tuesday, February 2, 2021 at 3:00 p.m.**

A link will be posted on our website and we hope you will be able to join in!

We will have giveaways for members on this day at our offices up until 2:00 pm, while supplies last. Please stop by and see us!

OFFICE CLOSINGS:

Dr. Martin Luther King, Jr. Day
Monday, January 18, 2021

Annual Meeting:
Tuesday, February 2, 2021
Offices Close at 2:00 pm

Presidents' Day
Monday, February 15, 2021

IRS Warns People About a COVID-Related Text Message Scam

The IRS is warning people to be aware of a new text message scam. The thief's goal is to trick people into revealing bank account information under the guise of receiving the $1200 Economic Impact Payment.

Here's how this scam works. People get a text message saying they have "received a direct deposit of $1200 from COVID-19 TREAS FUND. Further action is required to accept this payment – Continue here to accept this payment." The text includes a link to a phishing web address.

The fake link appears to come from a state agency or relief organization. It takes people to a fake website that looks like the IRS.gov Get My Payment website. If people visit the fake website and enter their personal and financial account information, the scammers collect it.

Anyone who receives this scam text should take a screenshot and include the screenshot in an email to: **phishing@irs.gov** with the following information:

- Date/time/time zone that they received the text message
- The phone number that received the text message.

The IRS doesn't send unsolicited texts or emails. The agency will never demand immediate payment using a gift card, prepaid debit card or wire transfer or threaten to have a taxpayer arrested.

Visit Our Website

www.myghsfcu.coop

Remember to check our website for promotions and information that may not be announced in our newsletter.

Our Mobile App:

GHS FEDERAL CREDIT UNION
MyGHSFCU

Planning a Move?

Don't Move–Without Us!

As you get ready to move, please don't forget to tell the credit union how to reach you. Members who move to parts unbeknownst to us may someday face an unpleasant surprise simply because important information relating to their account or their taxes could not be mailed to them. Please let us know your new address so you can continue to receive important account information.

In addition, if your e-mail address changes, please be sure to provide us with your new e-mail address so that we can continue to get your statements to you. You can update your e-mail address online through Netbranch or you can visit a branch at your convenience. And don't forget about your children's accounts as well!

Remember, if you change your mailing or e-mail addresses and don't tell the credit union, we will not have your current information on file.

To ensure delivery notification, please provide us with a personal email address and not an email address provided by your employer.

Everything You Need to Know About "Smishing"

Author: Mandy Remke

What is "Smishing"? SMS phishing, known as "smishing," is a phishing attack through SMS messaging. These attacks look like text messages from reputable companies that ask their targets for personal information or to click a malicious link.

98% of SMS messages are read within one second of being received. This statistic makes SMS phishing very attractive to scammers and hackers. SMS phishing has been on the rise due to the rapidity of text messages and the simple fact that most people own smart phones with the capability to fill out information and click links. Many businesses and institutions have started sending confirmation links and messages through SMS. Cyber criminals have taken advantage of this and turned it into an easier way to breach personal information and businesses' confidential data.

Defend Against Smishing – The importance of education and prevention against SMS phishing attacks and breaches is just as important as any other cybersecurity measure that you are already taking. These attacks can be even less suspicious than email attacks and other forms of cyber security breaches because they are becoming so common and people are so quick to open them. Hackers will use your financial institution or mailing service to send messages that look legitimate to you. Beware of unsolicited text messages that appear to come from a financial institution or mailing service.

Cybersecurity practices against SMS phishing lines up with practices you take against email phishing scams. It is important to remember never to give out personal or financial information to unsolicited or unknown sources, especially over the phone. This cannot only put yourself at risk, but also your business or workplace. Employees clicking links that have access to company databases, company information, or even company emails can cause a breach.

Education is Key – Education, just like an email fishing scams, is the key to defending against SMS phishing attacks. Through cybersecurity training people will know how to handle SMS phishing scams when they do receive them. Many SMS phishing scams are disguised as financial institutions or even mailing institutions that feel official. Knowing the proper steps to take is crucial.

What should you do when you receive an SMS Phishing Scam? Some tips when it comes to protecting against SMS phishing line up nearly one to one with protecting against email phishing attacks. Traditional cyber security training for phishing attacks can translate over to training for SMS phishing attacks.

1. Never give out personal information.
2. Do not click unsolicited links.
3. Read the message closely. Check for spelling errors and grammar mistakes.
4. Look into the sender's telephone number. Check to see if the phone number matches the company's phone number. If you have received legitimate SMS messages from that company or institution before, check to see if the phone number matches previous messages you have received.
5. Check for verbiage such as "act fast" or sign up now or any language that is pushy, encouraging a quick action.
6. When in doubt, give a call to the institution to inquire.

Take Preventative Action – People give out information over the phone like they never have before and feel confident in smart phones' abilities to relay important information and important data. It is increasingly more important to focus on the cyber security side of mobile phones and smart phones to keep that information and data protected from cybercriminals.

Winter Loan Special

Take advantage of our Winter Loan Special which runs through April 15, 2021! You may borrow up to $5000. GHS FCU will give away a $50 Visa Gift Card to one lucky member each month through April, 2021.

Term of Loan Options:

- Up to 36 Months **at APR:**As low as 5%*
- Up to 48 Months **at APR:** As low as 6%*
- Up to 60 Months **at APR:** As low as 7%*

Congratulations to:

Taylor Rawls, for recently winning a $50 Visa Gift Card!

* APR (annual percentage rate) will vary depending on individual creditworthiness and the credit union's underwriting standards. A 36 month loan with 5.00% APR (annual percentage rate) would have monthly payments of $29.97 per thousand borrowed. A 48 month loan with 6.00% APR (annual percentage rate) would have monthly payments of $23.48 per thousand borrowed. A 60 month loan with 7.00% APR (annual percentage rate) would have monthly payments of $19.80 per thousand borrowed.APR (annual percentage rate) would have monthly payments of $19.80 per thousand borrowed.

DON'T FORGET:

- Receive a .25% APR loan discount on vehicle purchases through our car buying service with AAA! You will also get a free one year basic AAA membership with your loan.
- Each time you use your G.H.S. FCU Visa credit card you earn valuable ScoreCard bonus points toward gift and travel awards!
- Notify the credit union when traveling out of state or out of the country as the credit union is monitoring some out of state and all international transactions for potentially fraudulent activity.
- We can refinance vehicle loans!
- We can match rates!
- Loan applications can be submitted online.
- E-statements can be accessed directly from Netbranch.
- Try our mobile app!
- Ask for Kasasa!!
- See us for home equity loans or first mortgages.
- Sallie Mae student loans are available at your credit union (undergraduate and graduate).

Please call any of our offices if you have any questions or need assistance.

Winter Auto Loan Special

Rates are as low as 1.99% APR* for 36 months and as low as 2.50% APR** for 48 months. This rate is good for both new and used vehicles. Offer excludes existing loans with GHS FCU and no other discounts apply to this special. This offer expires April 15, 2021.

The APR will vary depending on individual creditworthiness and the credit union's underwriting standards.

*A 36 month loan with 1.99% APR (annual percentage rate) would have monthly payments of $28.64 per thousand borrowed.

**A 48 month loan with 2.50% APR would have monthly payments of $21.92 per thousand borrowed.