

## SMiShing Attacks

There have been recent reports of SMiShing attacks (also known as text phishing), which have impacted cardholders of financial institutions located primarily in the eastern region of the U.S.

As you may know, SMiShing is a type of social engineering that uses cell phone text messages to persuade victims to provide personal information such as card number, CVV2 (the security code on the back of your card), and PIN. The text message may contain either a website address or more commonly, a phone number that connects to an automated voice response system, which then asks for personal information.

The following are **examples** of SMiShing messages recently sent to cardholders:

- Text message originating from either [notice@jpecu](mailto:notice@jpecu) or [message@cccu](mailto:message@cccu):
- ABC CU- has- deactivated-your-Debit\_card.  
To-reactivate-contact:210957XXXX
- This is an automated message from ABC Bank. Your ATM card has been suspended. To reactivate call urgent at 1-866-215-XXXX
  
- Text message originating from [sms.alert@visa.com](mailto:sms.alert@visa.com):
- [sms.alert@visa.com/VISA](mailto:sms.alert@visa.com). (Card Blocked) Alert. For more information please call 1-877-269-XXXX.

**Please do not provide any personal information to anyone claiming to be your credit union and asking for CVV2 or PIN information. Please remember that Etowah Valley FCU will never ask for any personal information, including your CVV2 or PIN information.**

---

## IMPORTANT FRAUD ALERT: Recent Telephone Scam

Etowah Valley FCU has recently learned of a telephone scam attempting to obtain cardholder information. Please see details of this scam below:

### Event Characteristics

Cardholders have received computer-generated calls claiming to be from their financial institution. The calls claim their accounts have been frozen and then direct the cardholder to call a toll-free number to leave their debit card information in order to reactivate any cards. The toll-free number includes a recorded message that asks the member to key their account number, card expiration date, and PIN.

### Recommendations

- Make sure you [*i.e. cardholder*] initiate the contact, and the institution verifies your identity with questions only you would know.
- To verify whether a call is legitimate, call us or visit our website, using phone numbers or internet addresses from your credit union statement or account documentation. **Do not call back a number provided over the phone or click on a link in an email.**
- Most communications will include something that will concern or excite the victim.
- If you have been the victim of a scam, file a complaint at local law enforcement.
- Notify your financial institution.

If you have questions, please [contact us](#).

---

## PHONE FRAUD PHISHING SCAM ALERT!

A GA credit union notified GCUA this morning that a phone # from Canada is auto dialing phone #s in their area of GA. The message that is left is- "This is the security alert team for XYZ CU. Your card has been blocked due to recent activity that could have been fraudulent. To have your card re-activated, call 819-536-6014." When you call that #, it asks for card # and PIN to re-activate the card. Obviously, no CU would ever ask for this info by phone. This is a phone fraud phishing scam.

So far, this CU has received numerous member and non-member calls regarding this phone scam this morning. **If your credit union is targeted by this phone scam, please let us know ASAP.**

This credit union has reported this scam to GCUA, local law enforcement, FBI, NCUA, CUNA Mutual and their card processors. They are crafting a security alert for the front page of their website. They are working to create a consistent message to members and non-members calling in speaking to their staff.

---

## **IMPORTANT FRAUD ALERT: Recent Email Phishing Scam**

Etowah Valley FCU recently learned of a new phishing email titled "2008 Security Update Notification." Here's how it works: The email claims to be from **Verified by Visa** and instructs the member to enter their card number to "activate" their account on the Verified by Visa website in order to protect them against fraud while shopping online. **This is not coming from Verified By Visa. It is a fraudulent e-mail. Please do not respond to it.** Visa or MasterCard will never ask you for personal information by e-mail or telephone. These types of phishing emails look official and could easily be mistaken as legitimate. It's the holiday season and many of you are shopping online, please be aware that the crooks are hard at work. If you receive anything you think is suspicious, **please** forward it to [michelle@evfcu.com](mailto:michelle@evfcu.com). **Never reply to emails requesting YOUR FINANCIAL INFORMATION.**

---

## **Don't Get Lured In by Phishing Scammers**

Etowah Valley FCU is aware of a recent email fraud attempt known as phishing that generated multiple copies of an email message to members and non-members. This phishing scam directs individuals to a false website and asks for GA/FL United Methodist account information and other personal information. These emails were not sent by GA/FL United Methodist Credit Union and there has been no breach of credit union information. This is a phishing scam - delete the messages. If you are a member and have responded to one of these emails, **Call Etowah Valley FCU** immediately so that we may take further steps to protect your accounts. Etowah Valley FCU will never send emails requesting members to submit account or personal information. Please read further to gain insight on how to protect yourself against Phishing.

### **Internet Phishing**

There's a new type of Internet piracy called "phishing." It's pronounced "fishing," and what these thieves are doing: "fishing" for your personal financial information. What they want are account numbers, passwords, Social Security numbers, and other confidential information that they can use to loot your checking account or run up bills on your credit cards. In the worst case, you could find yourself a victim of identity theft. With the sensitive information obtained from a successful phishing scam, these thieves can take out loans or obtain credit cards and even driver's licenses in your name. They can do damage to your financial history and personal reputation that can take years to unravel. But if you understand how phishing works and how to protect yourself, you can help stop this crime.

**Here's how phishing works:** In a typical case, you'll receive an e-mail that appears to come from a reputable company that you recognize and do business with, as your financial institution. In some cases, the e-mail may appear to come from a government agency, including one of the federal financial institution regulatory agencies. The e-mail will probably warn you of a serious problem that requires your immediate attention. It may use phrases, such as "Immediate attention required," or "Please contact us immediately about your account." The e-mail will then encourage you to click on a button to go to the institution's Web site. In a phishing scam, you could be redirected to a phony Web site that may look exactly like the real thing. Sometimes, in fact, it may be the company's actual Web site. In those cases, a pop-up window will quickly appear for the purpose of harvesting your financial information. In either case, you may be asked to update your account information or to provide information for verification purposes: your Social Security number, your account number, your password, or the information you use to verify your identity when speaking to a real financial institution, such as your mother's maiden name or your place of birth. If you provide the requested information, you may find yourself the victim of identity theft.

## How to Protect Yourself

- **Treat the e-mail with suspicion.** Never provide your personal information in response to an unsolicited request, whether it is over phone or over the Internet. E-mails and Internet pages created by phishers may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to denote a secure site. If you did not initiate the communication, you should not provide any information.
- **Do not reply to the e-mail or respond by clicking on a link within the e-mail message.** Georgia Florida United Methodist FCU will never ask you to provide any kind of confidential or financial details via an e-mail request.
- **Contact Etowah Valley FCU as soon as possible to report the suspicious e-mail.**
- **Never provide your password over the phone** or in response to an unsolicited Internet request.
- **Review account statements to regularly** ensure all charges are correct. If your account statement is late in arriving, contact your financial institution to find out why. If your financial institution offers electronic account access, periodically review activity online to catch suspicious activity