NOTE: *Fraud attacks continue to evolve and increase, with losses in the billions of dollars over the course of a year. And yes, it happens to our churches. Just about every month I am hearing about a church that has discovered charges on their statement that they did not authorize. Some churches have lost hundreds and even thousands of dollars. Fraud may be inevitable, but financial loss is not, and here are tips that, if followed, can help you ensure the safety of your church's money.*

Important: If any of the following has happened or is happening to you, your computer or your bank account, contact me. Right then. Putting it off is inviting loss.

1) Bank Fraud – the most effective tool in the fight against bank fraud is monthly bank reconciliation. *(Tutorial #3505)*

- **Reconcile your bank accounts every month without fail**, so that any fraudulent charges are quickly discovered, reported and reversed. If reported after the grace period that your bank gives (which varies, but can be as little as 30 days), full recovery of the stolen funds may not be possible, which means your church has lost that money. *(Tutorial #3520)*

  The days of consistently being one, two or three months behind in your church's financial recordkeeping with no risk to your church, are gone. If you are a month or more behind, even if you eventually reconcile, your church's money is at risk. Checking accounts, debit accounts, credit card accounts, whatever you have, reconcile it. As soon after the first of the next month as possible. Report any unauthorized entries immediately. Don't wait days or weeks. The money that is lost may be your church's.

- **Use strong passwords for your bank account logins**. Don’t use the same password for all logins, and keep your list of passwords in a safe place, not on a sticky note on or next to the computer itself. *(Tutorial #5510)*

- **Don't click on or reply to unsolicited texts or emails that are asking for information about you or your bank account(s).** Period. Especially if they are telling you to click something or call a number or do something "RIGHT NOW" to save you from something awful. If you have any question about a text or email, or even a call from "your bank" asking for account number or login information, don't tell them anything. No matter how legitimate they sound. Hang up and call your bank directly, using an official bank phone number. Or contact an auditor and we can help you verify it.

- **Church bank accounts should not be accessed or registered on your personal computer**. If a personal computer is compromised, church assets can be lost.

2) Protecting the Treasury Computer

- **Password the computer:** We recommend that the computer have an access password, to keep the private information safe if the computer is stolen. If you create a new password for your computer, make sure that an auditor and/or someone in your church knows what it is. Because if you pass away suddenly and no one knows the password, all church data will be lost. A password on Jewel is a good idea too. *(Tutorial #5510)*

- **Use the treasury computer for treasury use only.** The more time the treasury computer spends online, whether browsing, streaming, gaming, school or personal finances and emails, the more chance of cyber fraud. Limit online exposure by using it only for church related tasks like Jewel, bank transfers, paying online bills and for Adventist Giving. You may need to access your personal email if treasury emails are being sent to it, but don't use the treasury computer for the rest of your personal correspondence. *(Tutorial #5560)*

- **Make sure the computer is updating Windows when it needs to.** Restarting your computer when you get a message that a restart is needed, or powering it all the way off at least once a week will give Windows time to install important updates, including anti-virus updates. If you are not sure you know how to do this, ask for a demonstration.

- **Virus Protection options:** Defender Antivirus is free and comes already loaded on your computer. You will not need to purchase an additional virus protection software.

- **Backup your data regularly.** Whether from fraud or power loss or computer malfunction, losing data is always traumatic. If you enter offerings and checks into Jewel once a month, a monthly backup is fine. But if you enter data all month long, backup on a USB drive after every use so that if something happens, your data is not lost. And store that USB drive in a safe place. Don't leave it in or next to the computer.

3) CYBER Fraud Awareness

- **Be on the lookout for suspicious links, attachments and downloads.** If an email comes from a source you don't recognize, or asks you to do something right away, offers something that sounds too good to be true, or needs personal information, think before you click. And when in doubt, do NOT click. Ask an auditor for assistance if you are not sure.

- **If a scary, weird or loud screen pops up on your computer,** telling you that you have a virus and that you need to click on a link to get help, immediately hold the power button down for at least 30 seconds and don't restart the computer until you have contacted me. I can make sure you get the help needed to ensure that everything is cleaned up before you use the computer again.

- **Email safety.** For multiple reasons, we suggest having a church Gmail address for all treasury email rather than using your personal email address. *(Tutorial #5510)*

- **Password Management:** Password breaches and leaks happen frequently. If your passwords are written and posted next to or on the computer, or if you are using the same username and password over and over, please reconsider your approach. For password management tips, *(Tutorial #5510)*

- If you know how to do it, keep a copy of your password list on the USB drive you use for backing up Jewel. If you do not, *Tutorial #5510* has password storage tips.

- **“Tech Support” Fraud.** "Tech Support" phone numbers or websites can look legitimate but can be scammers in disguise, trying to gain access to your information and bank accounts. If you are having trouble with the computer or a printer, and you do an internet search and click on a link where some online person volunteers to link with your computer to "help" you, stop, hang up the phone, shut down your computer, and call me. Right then. Sharing information with a faceless "help" person can end with them loading malware onto your computer, which could give them access to the church's bank account. A good rule of thumb is: Do not give anyone other than conference auditors or conference IT personnel access to the treasury computer. (or in cases of the need for computer repair, a legitimate repair person like the Geek Squad)

4) Mail fraud avoidance tips

- Invoices or bills that come to a church in the mail can be hoaxes, designed to scare you into sending them a payment. If you don’t recognize the sender, even if it looks official, don’t pay it. Ask for help to know if it is legitimate.

- Charges for yellow page ads are fraudulent. Invoices for domain registration with search engines are fraudulent unless you are paying the search engine (such as Google) for a preferred listing. Any charge for Web hosting should be checked with your Web master to make sure you are actually using that hosting service.

- Church directories, whether printed or online, should not be available to strangers – casual visitors to your lobby or website. They contain phone numbers and email addresses that scammers can use.

- Set up auto-pay on utility and other monthly payments. It is more secure than snail mail and also saves you time.

- If you mail payment checks, mail them in security envelopes that conceal the contents, and taking them to the slot inside the post office rather than putting them in your own mailbox for pickup is considered to be safer as well.

Corresponding videos: 3.1 – Use of Treasury Laptop. Find at https://www.gccsda.com/auditing/10963
3.2 – Passwords – Online and Computer.
3.3 – email Address Management.

For more tutorials on FRAUD PREVENTION FOR CHURCHES, see section 5500 on the gccsda.org auditor webpage.

This information has been brought to you by the Georgia-Cumberland Conference Audit Team
Created by Linda McCabe. Edited 8/25/2025