Sisters and Brothers, come Lord Jesus, come! 11/12/2023

Covenant Life

- Our next Prayer Meeting is **TODAY** at 3pm where we will honor members and family members who have served our country.
- Our **Life in the Spirit Seminar** continues today after our gathering. Please continue prayers for the 30ish people that were prayed for last Sunday!
- We have launched our 2024 Stewardship Promise & Recommitment drive. Please discern what level of financial support the Holy Spirit is prompting and where you can serve Community and click here: 2024 Promise.
- GodsDelight.org content: Jubilee; Prayer Meeting audio, summaries, transcripts, & teachings.
- Your ongoing financial support to the Community is sincerely appreciated. Please donate online here or mail your donations to P.O. Box 225008 Dallas, TX 75222.

Reflection

In place of a reflection this week, I am sending information to help us protect ourselves from cybercrime. This is a challenging problem that is getting worse by the day and part of our practical care and concern for each other necessitates that we speak openly about the problem, offer protections, and then have the boldness to ask for help. As a Community, we are here for one other and this is not just spiritually but in everyday matters. Below are ten practical things we can do to protect ourselves. Please consider each and contact your Area Coordinator or me if you have any questions or if we can help you.

1. **Protect your identity** – Be on guard if anyone says you need to share your personal or financial information with them. If you did not initiate the call, hang up and call the company yourself. Never ever tell anyone where you were born or your date of birth.
2. **Secure personal information** – Do not keep all your personal information such as wills in one place. Maintain two copies of all important documents and files. It is suggested that one is at home in a fireproof waterproof safe and the other is in a bank safety deposit box or stored with a close family member.

3. **Safeguard yourself** – Consider not answering any call if you do not recognize the number calling you. You can return the call if the caller leaves a message. If you do answer, consider remaining silent until the other party says hello.
4. **Passwords** – Choose passwords for all your accounts that are unique. For any account that has financial assets in them, use a different more complex methodology. There is a suggested approach here.
5. **Two-factor authentication** – If available, enable a two factor feature for all your financial accounts. This will require a second step to logon where the institution will text you a code to ensure it is really you logging on. This becomes an extra safeguard against scammers that might somehow learn your username and password.
6. **Alerts** – If your financial account allows, set up alerts to notify you of account activity. Some institutions allow you to be notified if someone enters the wrong password on your account or transfers more than a specified dollar amount out of your account.
7. **Biometrics** – Take advantage of and enroll in biometric features on your mobile phone and laptop (such as fingerprint or facial recognition) to login since it is more secure than a username and password.
8. **Phishing** – Our email is bombarded every day with scammers attempting to trick us. There are two things you can do to minimize the chances of being tricked. First, look carefully at the address where the email came from. If it does not come from someone@company.com then be super suspicious. It is important to look carefully to ensure that the last two words are exactly the company name and ".com", no other characters. Secondly, hover over any links or look at them carefully to see if they are directing you to an address that ends with ".company.com". The second to last item should be exactly the company name (no other characters) and the last item should be exactly ".com".
9. **Secure your finances** – Do not trust anyone to invest your money because of statements they make about promised returns. Only utilize credentialed advisors.

10. **ASK FOR HELP** – If you are ever unsure about information in a letter, email, or phone call, write down the details and ask a trusted family member, your Area Pastoral Coordinator, or contact me. The same applies if anyone offers you something that seems to be too good to be true, or anyone asks for your bank information, or they request you to send them money or gift cards, or they claim that the health or welfare of your family is at risk, or anything else that seems suspicious. Never send money or give out your banking information. Please ask for help from your family or from the Community. We are here to help each other!

God Bless,
David