

Security Message for Community Church Members and Friends

NOTICE – Summer is Safety and Security season, including cyber security. Please be alert for telephone, email or text message scams where someone posing as an official of the IRS, a bank, or other institution, asks for your password or personal information. That is called “phishing.” **DO NOT RESPOND!**

Recently, three members or our staff and one member of the congregation were targeted by someone claiming to be Rev. Peggy Clarke, asking that the individual purchase \$100 pre-paid debit cards on some pretext, then email back a copy of the back of the cards, after scratching off the hidden PIN number. The exact same thing happened at All Souls UU and its minister last week. This is called “spoofing.” Again, **DO NOT RESPOND!**

There are plenty of other scams out there and plenty of scammers. There are ways to minimize the risk:

- **Change your email and account passwords at least every 90 days.**
- **Monitor your bank accounts and credit card accounts daily for unusual activity.**
- **Set call and message blocks on your mobile phone for unknown numbers that call repeatedly.**
- **Do not write your full social security number or full credit card number in the memo section of any tax checks or credit card repayment checks.**