FIRST COMMUNITY BANK
OF MOULTRIE COUNTY

FS-ISAC | Security Tips Newsletter

July 2025 | Issue No. 23

Be cyber smart to stay cyber safe.

It's Time to Discuss Passwords

Summary

Who owns the security of your information?

The answer is that *security is everyone's responsibility* – including you and the businesses that secure your email address online or physically. That may be a big group. Think about how often you log into a website using your credentials. Now, think about how often you reuse the same password.
Odds are, hackers are thinking about it. Between April 2024 and April 2025, in the US alone, security breaches gave threat actors access to 184 million consumer passwords, according to a recent *Yahoo Moneywise* article.

The cybercriminals obtained email addresses, passwords, and login links "tied to major platforms like Apple, Google, Facebook, Microsoft, and even government and financial services," according to the article.

Key Facts:

- The Identity Theft Resource Center (ITRC) Annual Data Breach Report recorded 3,205 cyber attacks (8.7 per day) leading to data compromises in 2024.
- 90% of dark web "access for sale" listings feature stolen logins, and 60% of Americans reuse passwords. More than four million people use 123456 as a password. (Spacelift)
- According to security researcher, Troy Hunt, 14,983,511,979 passwords and 888 websites have been identified as compromised.
- Has your email address and/or password been compromised? Find Out Now.

Those credentials can be used to obtain more information about the victims with the goal of accessing their banking accounts.

With so many entities in possession of your credentials, password security is something that you need to manage – but how? By arming yourself with knowledge and make your passwords hard to hack.

Baseline Security Tips

Start your security protocol by checking to see if your email address and/or password have been

compromised by using this **free tool**. This tool even tells you which breach is associated with your stolen passwords. Additionally, you can register to be notified when credentials have been compromised.

If you discover you need to change passwords – or want to take better ownership of your security – use these tips.

- The National Institute of Standards and Technology (NIST) recommends passwords of at least 12-16 characters. Some organizations, such as the Cybersecurity and Infrastructure Security Agency (CISA), recommend even longer passwords. At a minimum, passwords should be:
  - **Long**—at least 16 characters long (even longer is better).
  - **Random**—use a string of mixed-case letters, numbers, and symbols (the strongest!) or a passphrase of 4 –7 random words.
  - **Unique**—used for one and only one account.
- Use Multi-Factor Authentication wherever possible – especially when accessing websites linked to financial records.
- Frequently change your passwords using the above criteria.
- Never click on links or attachments in emails.

Common Email Themes

Speaking of emails, be aware of the techniques scammers commonly use in emails:

- Urgent messages
- Generic greetings
- Suspicious claims
- Unrealistic promises
- Threatening language
- Typos and grammatical errors
- Suspicious links
- Unsolicited attachments
- Requests for personal information:
- Impersonation of a legitimate organization

If You're a Victim?

Immediately change any passwords you might have revealed. Consider reporting the attack to IC3.gov and the police, and file a report with the Federal Trade Commission.

Getting Help

If you identify suspicious activity involving your financial institution, contact them immediately.

TLP WHITE

12120 Sunset Hills Rd, Reston
VA 20190