



# BENNY BANK

## Protect your banking info from Phil!

### Use Strong Passwords and Multi-Factor



Make sure your accounts have complex, unique passwords (a mix of letters, numbers, and symbols) and change them regularly. Enable multi-factor authentication for an added layer of security.

### Monitor Accounts

Frequently check your bank statements and transaction history for any unusual or unauthorized activity. Set up email or text alerts for every transaction, withdrawal, or login to check for any suspicious activity.

### Use Secure Networks

Only use trusted, updated devices with antivirus software to access your banking information. Avoid using public wi-fi when accessing your bank account or conducting transactions.

### Storing Details

Don't store your banking passwords or account numbers on your phone or computer unless encrypted. Always log out of your online banking account after completing transactions or checking your balance, especially on shared or public computers.

### Beware of Scams

Be cautious of unsolicited emails, texts, or phone calls asking for your banking details. Always verify the source before responding. When accessing your bank's website or app, the URL should start with "https://".

## RESOURCES

- [cisa.gov/shields-up](https://cisa.gov/shields-up)
- [usa.gov/scams-and-fraud](https://usa.gov/scams-and-fraud)
- [ftc.gov](https://ftc.gov)

[cyberhouserock.info](https://cyberhouserock.info)