Protecting Your Email Account

At CommunityAmerica, our goal is to provide our members with the resources and information needed to keep you, your financial accounts, and your personal information secure. Part of this is protecting your online activity.

Your email is one of your most personal online accounts and keeping it secure is crucial to your privacy. We've broken email security into three phases that will help protect your account.

Phase 1

Prevention

Keep your account secure.

Use Strong Credentials

Your password should be unique for every online account, having at least 15 characters and containing a mix of letters, numbers, and special characters. Avoid passwords that are easy to guess.

Setup Multi-Factor Authentication (MFA)

MFA provides a second layer of security when attempting to access your email account by sending you a unique code via text or authenticator app with every login. This means that obtaining a password is no longer enough to compromise an email account.

Don't Send Confidential Information

Email is not secure. Never send sensitive information in an email, whether in the body of the email or in an attachment. Information can be viewed and used by unintended individuals if an email is compromised.

Phase 2

Early Detection

Stop fraudulent activity as early as possible.

Review Login History

This can show you the dates, locations, and IP addresses of devices used to access your account. If you see any that you don't recognize, delete it. Update your credentials.

Check Email Forward Settings

Fraudsters can use email forwarding settings to redirect incoming emails to another address. Delete any unrecognized filters.

Review Email Folders Regularly

Fraudsters can create new email folders and have messages directly routed there instead of your inbox. Check your "sent", "deleted", and all other email folders regularly for any unusual messages to/from your account.

Phase 3

Account Recovery

Regain control of account after it has been compromised.

Change Your Credentials Immediately

Change your password to something unique. Also, change the password of any accounts that may have used the same compromised password. Consider a password manager to help create and store your passwords.

Report the Compromise

Contact all financial institutions in which you have accounts. Request additional security be added to your account(s) such as security questions, passwords, account alerts, or MFA. Review your accounts for any unauthorized activity and report findings immediately.

Notify People You Know

Notify your friends, family, and anyone else on your email contact list that your email was compromised and to be cautious of any emails with abnormal requests or suspicious links.

If you have any questions or concerns regarding the security of your accounts, give us a call at **913.905.7000**, or visit **CommunityAmerica.com/Fraud-Prevention**, or stop by your closest branch.

CommunityAmerica® CREDIT UNION