Online Security

Quick Reference

Overview

ECCU takes the protection of your accounts and personal information very seriously. We start with ongoing staff training, advanced security systems, and proven processes. But our security is not complete until you understand the importance of your role in it.

Staff Training

Each ECCU staff member is required to complete security and privacy training soon after being hired. This initial training is followed by multiple refresher courses each year and annual reviews of security policies. Select departments also do additional training to ensure that staff members in those areas know how these policies affect their specific jobs. However, at the end of the day, it isn't the policies themselves, but rather ECCU's capable staff who value and care about your protection that makes the difference.

Security Systems

ECCU's security architecture involves multiple layers of firewalls, intrusion detection and prevention systems, data loss protection, fraud detection, and other tools designed to keep your information safe. Most of these systems work in the background and you'll never even notice them. But here are a few important security features that you may notice:

Encryption — ECCU's online systems use Secure Socket Layer (SSL) technology to encrypt your personal information, such as user IDs, passwords, and account information over the Internet. This prevents anyone from "eavesdropping" on your electronic communication with us.

You can confirm that your web session is secure by looking for a "closed lock" icon in your web browser window. Most web browsers use this symbol to indicate when a web page is encrypted for transmission. You may also look for the letters "https://" at the beginning of the website address. The "s" means that the web connection is secure.

Secure Passwords — We do not store your online banking password in a database anywhere. While the explanation of how this works is too complex to describe here, suffice it to say that your password decrypts a complex key on your PC that is transmitted to us. Your password is never sent to us so we don't know it, don't store it, and never have access to it. That's why you are asked to complete some extra security steps when you log in from a different computer. So keep your password secure and you can be confident that we will too. To change your password, sign on to ECCU Online and go to *Manage Profile*.

Security Systems (Continued)

Security Questions — ECCU requires online banking customers to select or create five security questions and provide answers. This "second factor" of security is used to confirm that it's really you at the keyboard any time our systems have reason to doubt (like when you're using a computer we don't recognize). It's important that you don't select questions and answers that someone could easily learn about you from a little online research. In fact, you can set up your questions to require a "wrong" answer as long as you can remember the wrong answer you set it up with. Your security questions and answers can also be changed by selecting *Manage Profile* in ECCU Online.

Timed Logoff — ECCU Online will automatically log you off after 10 minutes of inactivity. This reduces the risk of others accessing your information from your computer if you leave it unattended. But better yet, don't leave it unattended!

Proven Processes

Our handling of your assets and information are subject to regular scrutiny, not only by our internal staff, but also by third-party audit firms and government regulators. These reviews ensure that ECCU stays abreast of the new security threats that emerge every day. Included in these assessments and examinations are reviews of the controls and safeguards related to consumer privacy, which are described in our *Privacy Policy*.

Your Role

As you've read above, some of our security systems require your involvement to enable them so as to provide the best protection. Here are a few more things you can do to keep your accounts and information secure:

Strong Passwords — Most of us have too many passwords to remember easily, so using the same password on multiple systems is a common practice. That might be fine for your social media accounts, for example. But if Facebook, Twitter, LinkedIn, or (fill in the blank) gets hacked, do you really want your banking password to be compromised? Please do not use your online banking password on any other system.

Email Communication — Email sent to ECCU using the ECCU Online Secure Messaging system is secure. However, since other email (outside of ECCU Online) passes through unsecure servers on its way from sender to receiver, it is not secure and can be copied or intercepted prior to delivery. To maintain the security and confidentiality of your personal information, you should never include sensitive information in an email.

Please take these extra precautions when corresponding with ECCU via email:

- Reference only the last three digits of your account number or the last four digits of your card or Social Security number.
- Do not attach a completed form, application, or other document containing personal information.

Your Role (Continued)

Untrustworthy Links — Always go to ECCU Online either by typing online.eccu.org directly into your browser, using your own saved shortcut, or from the Online Banking link on www.eccu.org. Never use a link sent to you in an email or from an untrusted website. Fake emails and websites may be trying to lure you into giving up your password. Of course with ECCU Online, your password alone won't get them into your account since they need to know your security questions, have access to your computer or email account, or have some other way to compromise that second factor of authentication. But your password gets them one big step closer, so don't make it easy for them!

Be Aware — Always have your antenna up for anything that seems suspicious. Is there something that doesn't look right about that website or email? Then don't trust it. Know that there are people out there trying to trick you into clicking, typing, or just telling them what they need to know so that they can gain access to your accounts and personal information. By working together, we can keep your assets safe, secure, and under your control.