



## Online Security Tips

### Safe Web Browsing

- Use a current web browser. UCB suggests using one of the following 128-bit encrypted browsers:
  - Firefox (version 3.0.11 or greater)
  - Internet Explorer (version 7.0 or greater)

### Passwords

- Change your usernames and passwords regularly and use combinations of letters, numbers, and "special characters" such as "pound" (#) and "at" (@) signs. Protect your online passwords. Don't write them down or share them with anyone.
- Use different passwords for each application. Don't share passwords between applications.
- Do not use your Social Security number as a username or password.

### PC Maintenance

- Obtain the latest Windows Updates/Security Patches from Microsoft
- Regularly scan your PC for viruses, malware, or spyware. Keep virus protection up to date with automated updates from the various virus protection software vendors.
- Protect your answers to security questions you provided to the Bank. Select questions and provide answers that are easy for you to remember, but hard for anyone else to guess. Do not write down your security questions or answers or share them with anyone. If you have selected security questions on other websites, avoid using the same questions to protect your UCB online accounts. Please note that we will never ask you to provide answers to your security questions via email.

### Physical Security

- Keep your PC locked when away from desk
- Keep your PC screen out of view of general public
- Utilize a Window firewall to protect against intrusion (use built-in firewall if using MAC-OS, Windows XP or Vista). Free options include Zone Alarm.

### Daily Activity

- Avoid downloading programs, videos, or music from unknown sources.
- Don't open suspicious emails. If you don't know the sender, do not open email or any attachments. Send this email directly to SPAM or Bulk File folder. If you know the sender, scan incoming email first, then open. Ignore all SPAM emails.

- Never send sensitive non-public information via email unless the email is secured or encrypted.
- Use secure websites for transactions and shopping. Shop with merchants you know and trust. Make sure internet purchases are secured with encryption to protect your account information. Look for “secure transaction” symbols like a lock symbol (🔒) in the lower right-hand corner of your web browser window, or “https://...” in the address bar of the website. The “s” indicates "secured" and means the web page uses encryption. Prefer to use websites with extended validation indicating a green bar in the address field (note this will only display in IE 7.0 or higher, or Firefox 3.0 or higher):



- Always log off from any website after making a purchase with your credit or debit card. If you cannot log off, shut down your browser to prevent unauthorized access to your account information.
- Log off from online banking prior to browsing the internet.
- Close your browser when you're not using the internet.
- Log off your PC when you are done for the day.