SECURITY AWARENESS

Internet Scams

Be alert to common internet scams.

Phishing is an internet scam that involves an email which appears to be from a legitimate company, credit union, or government agency. The emails typically warn of a potential problem with your account, and request that you follow a link and provide personal information to update your account. You should NEVER reply to these emails, open any attachments, or follow any of the links provided.

Pharming is a type of fraud that involves redirection from a legitimate site to a site that appears to be legitimate, but has been created by fraudsters in an attempt to gain your personal or account information. Always be sure to access our internet banking site by typing the URL, www.boulderdamcu.org or www.bdcu.coop, into your browser.

Email Security

Email has become a quick and easy way to communicate with others; however, email is NOT SECURE. Never include personal or account information in an email as it can be intercepted and read by anyone having access to the servers on which it resides. Emails are like sending a postcard through the US Mail system.
Boulder Dam Credit Union will never ask you to provide any personal or account information via email. Remember, the credit union has your account information, so there would never be a need to request it from you or ask you to update it.

Login ID and Password

Your login ID and password for your online banking should be protected just as you protect other personal confidential information.

- Do not write down your login ID or password.
- Do not use the same password for your online banking that you use for other websites.
- Use a complex password that is not easily guessed. Do not include full names or information that is publicly available on public sites such as Facebook.
- Do not share your password with anyone.
- Change your password on a regular basis.
- Avoid storing or saving your password in software or applications.
- Be certain you are only entering your login credentials on our website, www.boulderdamcu.org or www.bdcu.coop.

Internet Security

Always password-protect your wireless internet connection. Be vigilant if you use public wireless internet access, as hackers and identity thieves have the ability to monitor these types of unsecured networks.

When engaging in any type of internet-based banking, check that the session is secure. Two indicators will tell you if the session is secure. One is the presence of https:// in the URL. The other is the presence of a digital certificate represented by a padlock or key in the bottom right hand corner or to the right of the URL text box at the top of the screen. If you double click on this icon it should provide you with information about the organization with which you have entered into a secured session.

PC Security

It is important to use and maintain up to date anti-virus software and install updates as they become available for your operating system. Ensure you also regularly patch Microsoft, Java, and Adobe products. These items are frequently updated because of vulnerabilities that have been found to exist within the software.

In addition to being protected by use of up-to-date anti-virus software, you should also regularly use software to remove any potential spyware from your computer. In some circumstances, this can compromise your PC security. Current anti-virus software does not catch 100% of every virus.

Also, use a firewall. This can protect against potential hackers and prevent access to questionable connections.

Other resources for detecting and preventing identity theft:

- FDIC: Don't Be an On-Line Victim: How to Guard Against Internet Thieves and Electronic Scams
- US Department of Justice: What Are Identity Theft and Identity Fraud?
- Federal Trade Commission: OnGuardOnline