POTENTIAL THREATS TO ONLINE BANKING	WHAT IDAHO CENTRAL DOES TO HELP PROTECT YOU	WHAT YOU SHOULD DO TO PROTECT YOURSELF
Computer viruses, spyware, and other malware	ICCU utilizes anti-virus and other protection software on all systems and ensures that scans and virus definition updates are current.	Have updated anti-virus software on your computer. Enable routine scans and regular updates to ensure your computer is protected.
Outside computer intrusion	ICCU implements state-of-the-art firewall and intrusion prevention systems.	Ensure your personal computer's firewall is enabled and configured properly.
System & software security flaws (Microsoft, Adobe, Apple, etc.)	We routinely update our servers with the latest security updates.	Keep your installed software updated. Enable automatic updates for your operating system.
Unauthorized computer or account access	ICCU's systems require a strong password for access to online banking.	Keep your passwords secure. Routinely change your passwords and do not write them down. If needed, store your passwords in encrypted password software.
Phishing and Pharming fraud techniques	Visit the Security Center on iccu.com to read examples of the latest fraud techniques and how to protect yourself.	Never provide personal information via email. ICCU will never ask for your information in an email. Be cautious of links in an email and do not open emails you do not recognize.
Identity theft	We have partnered with an industry leader to provide multifactor authentication. You may be asked security questions when accessing your account from a computer we do not recognize.	Keep your personal account information secure. If using a public computer, be sure to log off when finished. Review your account statements and report any unauthorized transactions immediately. Perform an annual review of your credit history.