

| <b>POTENTIAL THREATS TO ONLINE BUSINESS BANKING</b>              | <b>WHAT IDAHO CENTRAL DOES TO HELP PROTECT YOUR BUSINESS</b>  | <b>WHAT YOU SHOULD DO TO PROTECT YOURSELF</b>   |
|--|---|---|
| Computer viruses, spyware, and other malware                     | ICCU utilizes anti-virus software on all systems and ensures that scans and virus definition updates are current.                                     | Have updated anti-virus software on your business computers. Enable routine scans and regular updates to ensure your computers are protected.                                     |
| Outside computer intrusion                                       | ICCU implements state-of-the-art firewall protection.   | Ensure the firewalls on your business computers are enabled and configured properly.  |
| System & software security flaws (Microsoft, Adobe, Apple, etc.) | We routinely update our servers with the latest security protocols.   | 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. You authorize the employees you want to have access to your business accounts. | Keep your passwords secure and update passwords routinely. If needed, store passwords in encrypted password software.   |
| Unauthorized ACH/Transaction origination                         | ICCU provides education and training to help you configure your system correctly.   | Ensure unauthorized employees are not able to originate ACH or other transactions for your business. Set appropriate permission levels. Conduct internal audits.                  |
| Employee fraud   | We provide education and training for best practices to help you avoid fraud.   | Establish dual control process for online account access. Perform internal audits and be sure to remove access of former employees. Conduct employee background checks.           |
| Phishing and Pharming fraud techniques                           | Visit the Security Center on <a href="http://iccu.com">iccu.com</a> 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. |