ASIAN BANK
亞洲銀行

# Online Security Information

## Secure online banking sign in

Ensuring the security of your personal information online is a top priority for us. When you sign in to Online Banking, your Access ID and Password are secure. The moment you click Enter and before your Access ID and Password leave your computer, we encrypt them using Secure Sockets Layer (SSL) technology. This ensures the privacy of communications between you (your browser) and our, Asian Bank, servers.

## Browser security indicators

You may notice when you are on our home page that some familiar indicators do not appear in your browser to confirm the entire page is secure. Those indicators include the small "lock" icon in the bottom right corner of the browser frame and the "s" in the Web address bar (for example, "https").

To provide the fastest access to our home page for all of our millions of customers and other visitors, we have made signing in to Online Banking area secure without making the entire page secure. Please be assured that your Access ID and Password are secure and only our, Asian Bank, servers have access to them.

## Consumer Security

Asian Bank is committed to protecting your online security. We offer these tips and best practices from Digital Defense on how to safeguard your accounts and privacy.

**Home Computer Safeguards**

Parents can ensure that the home computer provides safeguards.

- Keep computers in the family room rather than the child's bedroom. It is more difficult for offenders to communicate with a child when the computer screen is visible to other family members.
- Research filtering, blocking or website rating applications to provide adequate content control.
- Monitor your child's interaction with online friends, just as you would their real time friends. Anonymous Internet contacts may not always be accurate. A twelve-year-old female's Internet identity may actually belong to a fifty-year-old man.
- Talk to your children with Internet capable cellular phones about safe usage, and be sure to monitor the phone records.

**Away from Home**

Parents should also be aware that the home computer is not the only way for their children to access the Internet. They can use the unmonitored computer at a friend's house, their school, the public library, a club or even a coffee house. In addition, certain game consoles, handheld devices and mobile phones have the ability to connect to the Internet. For these reasons, it is important to openly communicate with your child to form healthy Internet habits.

- Talk to your child about potential online dangers and sexual victimization.
- Teach your children about responsible use of online resources. The online experience is far more than just chat rooms.
- Talk to your child's school, friends, and public library about putting safeguards in place regarding unmonitored Internet access.
- Teach your children the following:
    - Never arrange a face-to-face meeting with anyone they meet online unless a parent is present.
    - Never upload personally identifiable pictures. Pictures are easily altered and can be widely broadcast in unflattering ways.
    - Never provide any personal information such as real name, phone number, address, social security number, school name, etc.
    - Make sure their screen name does not reveal too much about themselves (do not use, name, age, hometown, etc.)
    - Downloaded pictures can include unwanted programs, viruses, or sexually explicit images.
    - Never respond to any messages or postings that are obscene, suggestive, harassing, or make you feel uncomfortable.
    - Not everything they see or read online is true.
    - Never post information they would not want others to see. They need to realize that once they post it, they cannot take it back. Even if they try to delete it, older versions often exist in cyberspace.
    - Flirting with strangers online can have very serious consequences. Many people lie about who they are. You may never really know with whom you are interacting.
    - Trust your gut feelings and report any suspicions. Immediately notify a parent, another adult, someone they trust, or even let the police know if they feel threatened or uncomfortable about any online activity. Prompt notification could prevent someone else from becoming a victim.

## Business Security

### Protect Your Business from Email Phishing

"Email phishing" is a scheme where a fraudster intercepts payment instructions from a legitimate vendor to a business customer, changes the payment beneficiary information, and instructs the unsuspected business customer to make payment to the fraudster's account instead of the vendor's account. The fraudster ends up with the payment while the legitimate vendor does not get paid.

We highly recommend that you implement the following best practices to protect your company from being a victim of this scheme:

- Do not take payment instructions or changes to payment instructions by email.
- If you receive payment instructions or changes to payment instructions by email, implement a callback procedure to contact your vendor or trading partner to verify the authenticity of the request.
- Implement a process that requires additional review and approval of changes to wire templates and payment beneficiary information.
- Never give sensitive data (like an account number or password) in response to an email request, instant message or on a social network.

These are proven and long standing fraud management and operating controls that are widely used by companies, including Asian Bank. In addition to the callback procedure above, we also recommend that you continue to use the additional recommendations below to protect your company:

### Protect Your Business from Other Threats

- Implement dual control to initiate and release funds transfers, where two employees and two separate computers are required to complete the transfer of funds, either through ACH or Wires transfer.
- Establish appropriate dollar limits for ACH and Wires transfer, limiting the exposure in case of unauthorized attempts.
- Do not open emails from unfamiliar sources, especially those with attachments or links to click on.
- Maintain current version of antivirus software, run virus definition updates and scan on a regular basis.
- Review employee's user online banking access periodically and remove former employees immediately.
- Make your passwords longer, use a combination of upper and lowercase letters, numbers and symbols.
- Check for signs that the webpage is secure - a web address starts with "https" and a closed padlock for example.
- Promptly review Wire, ACH or other transaction confirmations and make sure you recognize them. Notify the Bank immediately at (215) 592-1188 if you notice any discrepancy or error.

**Need more help?**

Please contact Customer Service at (215) 592-1188, Monday through Friday from 9:00 a.m. to 5:00 p.m. and Saturday and Sunday from 11:00 a.m. to 3:00 p.m. ET, or email us contact@theasianbank.com .