華美銀行
EAST WEST BANK

Fraud Protection Guidelines

Cybercrime and fraud scams are consistently on the rise, and you cannot rely on a single system or service to protect against online fraud risks. We urge our customers to adopt multiple layers of security, starting with the refinement of operational procedures, implementation of system controls, and the installation of IBM® Trusteer Rapport® and other security software to achieve as much protection as possible.

East West Bank offers these guidelines to help protect you and your business. Considering the potential financial losses, business disruption, recovery time and costs associated with fraud, implementing these security best practices is well worth the effort. By maintaining the proper tools and having various oversight measures in place, you'll be better equipped to prevent losses to your business.

Wire Transfers & Online Banking:

- **Verify payment information** with sender when notified via email for payment

  Call the email originator at a previously documented number (provided outside of the email) to confirm payment instructions are accurate. Fraudsters may attempt to send payment requests from an email account that is disguised to be from a known vendor. Fraudsters may also alter the original email instructions in order to reroute funds to the fraudster instead of the intended vendor. Be cautious of emails that stress urgency and secrecy. Look for slight variations in email addresses and subtle discrepancies.

- **Install IBM Security Trusteer Rapport**

  We provide this complimentary software to help you combat financial fraud. Trusteer Rapport's innovative technology picks up where conventional security software falls short. From the moment it is installed, Trusteer Rapport protects the customer's device and mitigates financial malware infections. It provides instant PC and Mac anti-fraud protection against financial malware, as phishing attacks.

- **Implement dual control (Bank's Standard Settings)** to initiate and release payment transactions on separate machines

  Having a minimum of two persons involved in a transaction ensures accuracy, and adds a layer of complexity for fraudsters and internal employees to compromise your accounts.

- **Establish appropriate company and/or user transaction dollar limits**

  This will help limit the exposure in case of unauthorized payment attempts.

- **Never disclose or write down usernames, passwords, and token passcodes**

  Never disclose these types of sensitive information to another party via phone, email, text, or chat; Bank personnel will never ask for passwords and token information.

- **Review full details** of the payment transaction before release

- **Promptly review Wire Transfers and other transaction notifications**

- **Setup email alerts** for Wire Transfer and balance thresholds

  Email alerts will help bring your attention to unauthorized transactions and unwarranted changes to your account balance.

- **Reconcile account activities daily**

- **Regularly review user access**

  Allocate permissions and access to staff on an "as needed" basis to manage risk and limit over privileged users. Promptly deactivate employee's access when it is no longer needed.

Continued on next page >>

華美銀行
EAST WEST BANK

Safe Computing:

- **Regularly scan and update to current versions of firewall/antivirus software** and related technologies (operating systems, browsers, and security suites)
  Security updates patch vulnerabilities that may be exploited by malware and help keep users and their data safer. You are only as protected as your system and security software updates.
- **Dedicate a computer with restricted internet access** to conduct financial activities (accounting, online banking, and outgoing Wire transfers)
  Restricting web surfing, email, and other access of the computer will help limit the exposure and possibility of infections.
- **Enhance your password security** by making your passwords more complex and usedifferent passwords for different accounts and systems
  Try combining random words together for easy remembering. Incorporate upper- and lower-case letters, numbers, and symbols. Do not use birthdays, family names, or telephone numbers.
- **Consider using false answers for security authentication questions**
  Fraudsters do their research, gathering public knowledge and detailed information before acting on their target. Using mixed or untrue information will help strengthen your accounts' security.
- **Do not open unrecognized email** and open familiar emails with caution. You can never tell who is truly behind the email
- **Email is not a secure medium of communication.** Encrypt sensitive data before sending
  Do not respond to any messages requesting the following information:
  1. Online banking credentials
  2. Personal information (Social security number, business TIN, mother's maiden name, and etc.)
  3. Bank account, credit card or ATM/debit card numbers
- **Destroy any emails** that contain your initial password
- **Disable 'AutoComplete'** or other memorize password functions on browsers
- **Avoid downloading attachments or clicking on embedded links in emails or websites** whether you are or are not familiar with them
- **Log off when you've finished your banking** or if leaving your computer unattended
- **Restrict access to computer functions,** including software installations, USB, and CD Burner
- **Use HTTPS websites**
- **Avoid connecting to unsecure Wi-Fi**
  Unsecure internet networks may allow fraudsters to intervene and steal information as it is being transmitted. Review your mobile device's setting to disable 'Auto Connect' feature to avoid connecting to unknown/unverified networks.
- **Avoid use of public computers** and unsecure internet connection

Accounts and Checks:

- **Utilize dual control** throughout your check stock storage, printing, issuing, signing and dispatching
- **Audit and destroy old inventory**
- **Be mindful of the information you are throwing into the trash**
- **Never write down your password** or allow anyone else to use your password.

Transaction Banking Services

Phone: +852.2218.9010
Email: CustomerCareHK@eastwestbank.com
Monday – Friday 9:30 AM to 5:00 PM HKT

TAKE CHARGE NOW AGAINST FRAUD AND CYBERCRIME.

Notify East West Bank Hong Kong Branch **immediately**, if you notice any discrepancy or require more information on fraud prevention.