Tips to protect every organization, every day.

Cyber crime continues to evolve and grow, resulting in billions of dollars in losses each year. Here are some tips to help you combat fraud and protect your organization from monetary losses, information breaches and damage to your reputation.

Mandate and enforce process controls

Such as segregation of duties and dual control when handling payments, sensitive bank information and personally identifiable information (PII).

Use secure and trusted internet connections

When conducting business and sharing sensitive information.

Regularly inspect credit agency reports

And state record databases to identify and fix any discrepancies.

Conduct background checks

On all employees and contractors who are authorized to handle sensitive data, as well as initiate and/or approve payments.

Review all bank accounts at least once daily

And reconcile frequently to identify any unusual debits or credits, including small dollar amounts that may seem negligible.

Reduce the risk of loss

By using fraud mitigation tools such as positive pay and ACH blocks/filters to prevent unauthorized transactions.

Be alert to emails that contain attachments or hyperlinks.

Although anti-malware and anti-phishing tools may block most malicious emails, it's best to be cautious since no single solution catches everything.

Notify the bank and law enforcement

If accounts and/or sensitive data have been compromised or seized. The bank can safeguard accounts from further exposure and restore services while the matter is investigated.

Verbally authenticate all changes

To payment requests and delivery instructions, especially those that require urgent and discreet handling.

Separate activity for payables and receivables

To allow better control over account transactions and easier reconciliation.

Watch out for emails claiming to be from legitimate sources if those communications are not typical.

Random and unsolicited emails should be scrutinized closely, since these are likely phishing attempts.

Build and promote a culture

Where fraud awareness and mitigation are second nature for the whole team. Educate employees about the different scams they may encounter from external threats and adopt measures to identify fraudulent transactions that may originate internally.

Remember: this is not a one-time exercise. Maintaining strong security procedures is an ongoing process and educating your teams should be approached in the same way.

TD Bank

America's Most Convenient Bank®