Your employees are your best defense against cyber fraud and theft.

Recent studies confirm that most cyber security breaches are simply caused by individuals making innocent mistakes – errors that could be prevented with the right tools and training.

The Human Factor

- 90% of POS breaches were related to weak passwords or weak remote access security
- 95% of all data breaches recognize human error as a contributing factor
- 90% of malicious software (malware) requires human interaction to work

The cost of data breaches for small businesses is expensive, and can exceed $50,000.

Risk is at an all time high. Follow the steps below to protect your business.

Creating a Culture of Cyber Security

Regardless of the size of your business, cyber security starts from within. By taking a proactive role, you and your employees can help protect your business from fraud, and at the same time, increase customer trust and loyalty.

Don't wait until it's too late. Connect with a TransArmor® Support Expert to get started. Call 866-359-0978 today!

How to Create a Culture of Cyber Security

Step One

TAKE CHARGE

- Make payment security a business imperative with strategies such as tokenization and encryption
- Invest the time and money necessary to set up and monitor security systems and processes
- Create standardized daily processes for ensuring security functions are working properly

Step Two

MAKE EVERYONE ACCOUNTABLE

- Set clear expectations for your employees of their role in protecting customer data and payment information
- Foster an environment that encourages honesty, and open dialogue about best practices and procedures
- Conduct spot checks on employee procedures, habits and behaviors

Step Three

TRAIN & REINFORCE

- Make security awareness part of new hire training
- Leverage educational resources
- Conduct refresher training regularly
- Educate employees of new fraud tactics and data breach threats
- Set milestones and reward incentives for exceptional security compliance

Step Four

CHECK UP ON YOUR DEFENSES

- Ask your vendors to regularly introduce advanced tools, and adopt new innovations quickly
- Develop an audit schedule for testing operational IT practices
- Take cyber security threats seriously
- Now is the time to take steps to protect the business that you've worked so hard to build.