51% of Mid-Sized Businesses Targeted by Cyber Fraud: TDA Provides Prevention Strategies and Fund Recovery

Cybercrime, including crypto scams and forex scams, identity theft, and phishing scams, are reaching an all-time high

SCHAUMBURG, ILLINOIS, UNITED STATES, July 22, 2021 /EINPresswire.com/ -- Cybercrime, including crypto scams and forex scams, identity theft, and phishing scams, are reaching an all-time high. To grasp the scale of the problem, if cybercrime were a country, it would have the third-highest GDP after China and the United States. In this environment, fund recovery services such as Trader Defense Advisory provide essential strategies for protection.

Although individuals and large corporations are often vulnerable to phishing attacks, malware, and ransomware, among the main targets are medium-sized businesses. Cybercriminals are like pirates on the high seas. They may ignore small boats because there isn't the potential for huge plunder. The large ships may have plenty of treasure, but they are well-fortified and hard to attack.

These cyber pirates target mid-sized ships which have enough treasure in the form of customer data and money in accounts to make the venture worthwhile, but less protection than the large corporations. TDA warns small businesses to take steps to prevent fraud and to consult with experts for fund-recovery if an attack has occurred.

Medium-Sized Businesses Under Attack:
Experts have estimated that a malware attack will happen to a business every 11 seconds by the end of 2021 with yearly losses of trillions of dollars. Half of the small to medium-sized businesses suffer from malware or ransomware attacks and 60% of the time, they go out of business within a year of the attack.

These attacks are happening, in part, because small to medium-sized businesses are not taking sufficient precautions to avoid them. They may not have advanced security anti-virus and anti-malware software installed. Increasing numbers of employees working at home may put data in danger if they don't work with updated versions of protective software

Best Practices to Avoid Cyber Fraud:
Employees of small to medium-sized businesses should be thoroughly trained to prevent

phishing attacks, according to TDA.

One common scenario that can be avoided is employees clicking on links, opening files, or downloading items that may contain malware. For instance, a worker receives an attachment from a client that is supposed to contain a document. Without thinking about it, they will download or open the document, see it is not the one expected and assume that it was a mistake. Once this happens, the malware will gradually infiltrate the system and will spy to find keywords, data, and sensitive customer information. The company may receive a message from the cybercriminal that all of the data has been apprehended and they must pay a certain amount to retrieve their data.

The company has not only lost access to essential customer data they need to operate their business, but the cybercriminals have gained access to this information and can infiltrate client accounts, use their credit card information and manipulate their bank accounts.

In this situation, the business may find they have no choice but to pay the ransom to regain access to their data. The threat has not ended with the payment of the ransom. Not only has the financial damage been done to their company, but customer information has been compromised. When this is discovered, they are likely to lose customers and fail to attract new ones. As a result of one malware attack, a business can go under.
Protecting Your Business and Recovering Funds
TDA urges business owners to upgrade to the highest level of malware protection they can afford. In addition, all employees must constantly be on the lookout for cyber fraud. They must adopt best practices such as not opening attachments or clicking links unless they are certain they are sent from a legitimate party.

Even when a company has to pay ransom to regain access to their network and data, business owners should never give up hope on fund recovery. TDA consults with individual and enterprise clients and commits their expertise to track down cybercriminals, working with law enforcement and regulators, and expediting the fund recovery process on behalf of clients.

About Trader Defense Advisory:

Trader Defense Advisory offers all clients a free consultation to assess their cases and design a roadmap for pursuing their claims. The TDA team works tirelessly to advocate for clients and will fight back against phishing scams, identity theft, crypto scams and forex scams.

Contacts:
Dan Arnheim, Media Relations Director
Trader Defense Advisory

Daniel A
TDAI Group, LLC

+1 917-920-6749
email us here
Visit us on social media:
Facebook
Twitter
