Online Fraud and Customer Logins

Securing User Access with Multi-Factor Authentication

Online logins allow your customers and partners to manage their bank accounts, health care information, and even order pizzas on through a website or portal. They are convenient and can also significantly reduce the costs related to customer service.

*Unfortunately this access is also an attractive target for hackers. To protect your customers and your business, every customer login access point should employ advanced Multi-Factor Authentication (MFA) to keep your data and systems secure.*

Many businesses have already learned the hard way, about the security risks associated with customer access logins and portals:

- **Oracle Corp.** confirmed to Krebs on Security that some of its systems including a customer portal supporting merchants using Oracle's Micros point-of-sale payment system have been breached, allegedly by a well-known group of Russian criminal hackers.

- A bug affected an internal customer care portal used by T-Mobile’s employees to access internal tools and look up customer account details. The password protection on the portal was insufficient.

- Centers for Medicare & Medicaid Services staff detected anomalous activity in the Federally Facilitated Exchanges Direct Enrollment pathway for agents and brokers. They believe that approximately 75,000 individuals’ files were accessed.
Confidence, not Compromise

Your business does not need to sacrifice customer experience for the sake of security.

Businesses benefit from the cost savings of self-serve customer portals. Customers are increasingly coming to expect this convenience.

Fortunately, with MFA solutions from SecurEnvoy, you can secure your customer portals without sacrificing savings for you or convenience for your customers.

Multi-Factor Authentication from SecurEnvoy is a cost effective means of securing access to your systems by employing additional verification beyond a simple user name and password.

When generating access codes SecurEnvoy’s technology splits the seed records into two parts so that hackers are unable to copy a key from a compromised device.

To ensure a convenient customer experience, SecurEnvoy offers a wide variety of code delivery options. Virtually any device can be used including mobile phones, desktop computers, and even landlines.

Our deployment options are made to suit the needs of your business and integrate with your existing technology systems.

Let’s Talk.

info@SecurEnvoy.com
(866) 777-6211