Bermuda Economic Development Corporation

Cyber Security Webinar Series:

Is Your Online Payment Platform Secure?

Ronnie Viera, **CISSP, CISM, CISA, CRISC, CertIoD**
Chief Operating Officer
First Atlantic Commerce Ltd.

Tricia Lines-Hill
Senior Vice-President
Marketing & Business Development
First Atlantic Commerce Ltd.

Disclaimer

All views and opinions expressed during this presentation are for educational purposes and are solely that of the presenters and not necessarily that of the presenter's employer or any other associated organization.

A little about us

- Ronnie Viera
  - 40+ years in IT & Cybersecurity
  - FAC & Payments – 20+ years
- Tricia Lines-Hill
  - 30+ years in Marketing and business
  - FAC & Payments – 20+ years

Agenda

- Cybersecurity
- Security for your web-store:
  - Site Administration
  - Personal and other data
  - Payment Process
- How to start the online store process
- Questions

Cybersecurity:

People, Processes & Technology used to protect systems & data from unauthorized access, use, disclosure, modification, disruption, removal and destruction

- *Confidentiality*
  - *Data is accessed/viewed by authorized persons only*
- *Integrity*
  - *Data is accurate, up to date*
- *Availability*
  - *Systems and data are available when they are needed*

Securing your web store

- **Reputation –** the store is the front facing image of your business so it is important to actively manage all aspects of the website

- **Shopping cart applications** – many small to medium sized businesses will use a cloud based service for hosting their web store – important to evaluate the vendor and capabilities of the software before selecting

- **Data** – the web store will have product, customer and financial data which must be secured properly as any event could cause a disruption to your business and have a financial impact

Securing your web store

Site Administration:

- **Set up ADMINISTRATOR access for all website configuration settings:**
  - **Site design**
  - **Inventory maintenance**
  - **Pricing and other financial parameters**
  - **User setup and maintenance**

Securing your web store

Site Administration:

- **User Access Controls:**
  - **Proper user authentication**
    - **unique user IDs for all staff**
    - **Complex passwords – special characters/alpha-numeric, min length 12 characters, expiry settings, no repeated passwords**
    - **Two factor authentication – text to phone, email, biometric**
  - **Authorisation levels – ability to configure access for users so that they have the minimum necessary for their role**

Securing your web store

Site Administration:

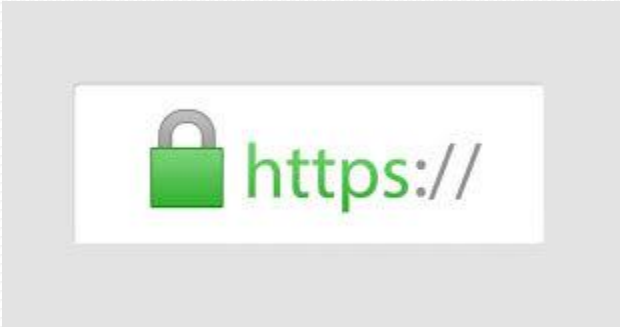
- **Security Awareness Training**
  - **Essential for all users**
  - **Very effective for preventing Ransomware attacks**

- **Backups:**
  - **Ensure that you take a backup of all website data regularly independent of the software provider or cloud service**
  - **Store the backup data offline i.e. not on your servers or workstation**

Securing your web store

Personal & Other data: "The Crown Jewels"

- **Customer data:**
  - **Collect** as little sensitive customer data as necessary
  - **Privacy laws -** be informed about Bermuda Privacy law (PIPA) and in laws of the countries where your customers are located e.g. European GDPR
- **Inventory data –** any private product information
- **Financial data -** product costs and pricing
- **Encryption** – at rest and in transit (SSL)



Personal Information Protection Act – PIPA

- Governs how sensitive data on a person is used and handled
- "Sensitive personal information" means any personal information relating to an individual's place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information.
- Any business storing or processing sensitive personal data will have to abide by the Act once it comes into force later this year.
- Start by carrying out a data inventory in your systems to determine what type of personal data you are storing; review the processes around collection and maintenance

Securing your web store

Payment process:

- **Card data:**
  - Considered sensitive data requiring appropriate security and handling at all times – encryption at all times
  - Hosted Payment Page - most shopping cart applications use a payment page hosted by the payment gateway
  - CVV2/CVC2 – 3 digits on the back of a card – must never store this data

- **3DS 2 – cardholder authentication process**
  - Risk analysis performed by the card issuer
  - Enter a PIN or Password or receipt of a text or email message to verify the card holder

- **Secure Sockets Layer/SSL Encryption** – secures all data transmission

Securing your web store

Payment process:

- **Fraud mitigation:**
  - Customer accounts – require that customers set up an account – reduces the risk of fraud
  - Fraud Management service – usually offered by the payment gateway
  - Address Verification Service (AVS)

How to get started?

- **Merchant Account – HSBC, Clarien, Butterfield**
- **Payment Gateway – integrate to our platform.** We are the interface between a merchant's website and the merchant's acquiring bank
- **Shopping Cart software --- plugins are available for various shopping carts**
- **Integration and testing**