# TIPS TO SECURE YOUR ONLINE BUSINESS



**Educate Your Customers**: Security is a shared responsibility. However, your customers might not be aware of this. You must educate your customers on their responsibilities. Customer education and awareness must be consistent and should not adversely impact the overall customer experience.

**Secure The Identity**: The identity is often the point of most friction for the customer, and therefore an area that warrants thorough consideration. At minimum, your platform must support Multi-Factor Authentication (MFA) and enforce a strong and complex password policy (for customers and administrators).

**Protect Customer Data**: If you do not need the information to facilitate a transaction or satisfy a regulatory requirement, do not collect the information. The Protection of Personal Information Act (POPIA) requires that all personal information that is collected and processed must be adequately protected.

**Use Secure Hosting Providers**: The security of any ecommerce platform is directly impacted by the level of security of the hosting provider. Typically, hosting providers offer a range of security features. Consult a security professional and ensure that you include the appropriate security feature for your business.

**Use an SSL Certificate**: Without an SSL certificate, your website will display an "insecure" warning to visiting customers. There are a host of good technical reasons why an SSL certificate is required. Your hosting provider is likely to offer this at a cost. This is on-negotiable.

**Keep Software Updated**: Software is inherently insecure, and software vendors regularly release software updates, also known as software patches. It is essential to update applications and hosting platforms to protect your ecommerce website from cyber threats.

**Use PCI-DSS Compliant Service Providers**: The processing of payment card data is regulated, and depending on the volume of transactions, the Payment Card Industry Data Security Standard (PCI-DSS) may apply to your organisation. Ensure that you understand your PCI-DSS obligations and only use PCI-DSS compliant payment gateways.

GRANT HUGHES
SPEAKER - AUTHOR - ADVISOR

CyberAwareness
Influencing change, one message at a time