From: ANZ
To: edmsamples@lasercomp.com.au
Subject: Important information from ANZ to help you protect your business against fraud.
Date: Wednesday, 3 May 2017 3:59:47 PM

Dear ANZ Merchant,

From time to time ANZ will send important information to help you protect your business against fraud. A copy of this email is also available on our website, please visit www.anz.com/merchant-security.

This email contains an update for merchants using the **Magento®** eCommerce platform. Please share this with web development and IT service providers that help maintain your eCommerce website.

Please Note: This email is not advice and contains general information only regarding the protection of card data. It does not take into account your business' particular requirements. Please contact your web developer and IT service providers of your online store if you require specific assistance.

Magento® eCommerce platform

Magento® has published critical security updates and we recommend you take the following actions immediately, to help protect your business:

- Install up-to-date security patches via Magento® Security Centre https://magento.com/security
- Sign up to receive alerts about security and new patches https://magento.com/security/sign-up
- Find out how to remediate your site after a malware attack https://magento.com/security/best-practices/remediating-your-site-after-malware-attack

ANZ requires you to protect card holder data

We have seen a significant increase in card data stolen from merchant websites and subsequently used to make fraudulent purchases with other merchants.

By implementing these minimum requirements you can significantly reduce the risk to your business:

- Integrate your website with a payment gateway where the card data is keyed into a Payment Card Industry Data Security Standard (PCI DSS) compliant payment gateway's hosted page or iframe, removing the risk of card data being stolen from your website

OR

- Immediately action critical security updates for your website
- Install a managed firewall to help protect your business from external attack
- Effectively manage user access and passwords: change any default or vendor passwords; ensure passwords are complex (i.e. use combinations containing capitals, lower-case, numerals, and special characters, minimum 8 characters, etc.); and regularly change your passwords
- Regularly test the security of your website using vulnerability scans and penetration testing - fix any high-risk issues you identify during testing
- Ask your web developer and IT service providers how they can help strengthen security for your eCommerce website

By taking action you can maintain focus on sales and not on eCommerce fraud and help customers feel confident shopping at your online store.

Payment Card Industry Data Security Standard (PCI DSS)

Payment Card Industry Data Security Standard (PCI DSS) is a set of security requirements established by the major card brands Visa, MasterCard, American Express, Discover and JCB to protect card data. All merchants and service providers should be PCI DSS compliant.
PCI Council website https://www.pcisecuritystandards.org/.

Please Note: This email is not advice and contains general information only regarding the protection of card data. It does not take into account your business' particular requirements. Please contact your web developer and IT service providers for your online store for further assistance.

Frequently Asked Questions

1. Why should I upgrade to the latest security updates from Magento®?

Cyber criminals invest in technologies that trawl the web to find the weakest link. Online stores which are not protected become an easy target for them.

2. How do I know if I have been a target?

Your customer or ANZ may determine fraud has occurred after shopping at your online store. Check that website file sizes are exactly the same as those uploaded originally. Increased file sizes may indicate that additional lines of code have been injected to extract card data from your payment page. Talk to the service provider who built your online store if you need more information or support.

3. How can I help to protect against card data being stolen through my online store?

Ensure you are using validated service providers who are compliant with the Payment Card industry Data Security Standard (PCI DSS). If you haven't already done so, you can reduce the chances of having card data stolen by migrating your payment page to an iframe solution, provided by a compliant gateway. This integration is considered 'best practice' and highly recommended by the PCI DSS Council.

4. How can I validate if a service provider is PCI DSS compliant?

Service providers who have been validated by an authorised assessor are listed on the approved Visa and MasterCard website service provider lists.

- Visa Service Provider List
  http://www.visa.com/splisting/
- MasterCard Service provider list
  http://www.mastercard.com/us/company/en/whatwedo/complaint_providers.html

5. Do I need to be PCI DSS compliant if my service provider is?

Everyone is responsible for protecting card data, PCI DSS is the industry standard for merchants and service providers. Discuss with your service providers what security components they believe you are responsible for. Service providers include your developer, shopping cart, payment gateway and hosting provider.

6. How can I find more information about card data security?

If you need help, contact the web developer and IT service providers who helped build your online store. Seek their assistance with maintaining your eCommerce website security.

- ANZ Guidelines for Securing Cardholder Data for your eCommerce Website
  http://www.anz.com/website-card-security/
- ANZ Merchant Security
  http://www.anz.com/small-business/products-services/merchant-services/merchant-security/
- PCI Council create the security standards for card data
  https://www.pcisecuritystandards.org/

7. What if you believe card data has been stolen from your online store?

Immediately alert ANZ Merchant Services on 1800 039 025. ANZ can assist you with remediation and report potential cards at risk in an attempt to minimise further fraud.

8. How can I tell if I am using the Magento® eCommerce platform/shopping cart?

You will usually be able to see the provider of the eCommerce platform/shopping cart of your website where you login to update your product listing. Alternatively, contact your web developer/IT staff who assisted in setting up your eCommerce website.