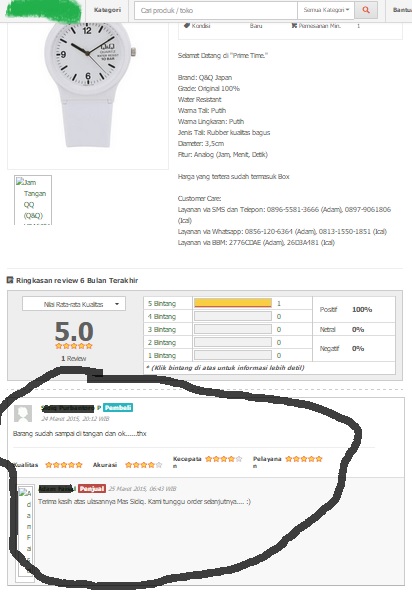
1. *How to prevent us from cyber criminal?*

* Education and training
* Do all your employees understand the most common hacking tactics, such as phishing, social engineering, or packet sniffing (to name just a few)?
* Education and awareness across your staff will go a long way to protect yourself against many types of cybercrime.
* **Securing Computers, Digital Assets, and Networking**
* Is all software housed within your network continually up to date? Exploits in software are very common ways hackers gain access to systems and sensitive data. Updating software on network-connected machines should always be a top priority.
* Do you have business-class antivirus software installed (and up to date) on all office workstations and servers? Leading antivirus software can detect, remove, and protect your machines and network from malware.
* Do you scan your [website or web applications](http://www.thesba.com/web-services/)for malware? Many of us are used to checking for viruses and malware on our personal computers, but don’t realize that websites and web applications are just as susceptible.
* Do you have reliable backups of all of your critical [data](http://www.thesba.com/web-services/cloud-managed-services/)? Recovering from many types of common cybercrimes often involves restoring your data from a point prior to the event in question. Not having reliable and securely stored backups of your data is a significant liability.
* Is your network equipped to handle network-specific attacks? Earlier, we mentioned a common type of network attack called a DDOS. Unsophisticated networks are particularly susceptible to these, as DDOS mitigation devices and tools often require enterprise-sized budgets. If you own a small business, this type of luxury wouldn’t normally be practical, financially speaking. However, with the growing adoption of [cloud and utility computing services, using a quality cloud-computing partner](http://www.thesba.com/web-services/cloud-managed-services/)— one that has already invested the necessary capital to protect its network—is a cost-effective solution.

*Source:* [*http://www.forbes.com/sites/thesba/2013/08/28/how-to-prevent-cyber-crime/*](http://www.forbes.com/sites/thesba/2013/08/28/how-to-prevent-cyber-crime/) *with a little bit alteration*

* Do not open any link from the email you got. Especially the suspicious email. Because these are a phisher, cracker, malware threaten us there. Update your anti virus for routines to prevent this
* If you want to transaction on the e-commerce website. Observe the comment below the thing you want to buy like this



If you didnt see the comment below the item you want to order it possibility a deceiver. Deception like this usually happen in the social media like facebook or Instagram. And very seldom was found on the spesific e-commerce website If you find a phenomena like this please contact the seller about the item their sell.

* Careful if you had a transaction with a credit card/ATM because this cyber crime was called Cyber Carding. This is some way to prevent the cyber carding:
* Secure your username and password

Username must use your real name so that be easier in the data process, use the unpredictable password. Do not use your birthday as the password or any relation with your family

* Carefull when doing a transaction

Try to always aware when your card being process in the bank, mall, or shop. And keep safe the receipt. The receipt may not missing. Match with the credit card/ATM billing when the payment

* Wifi could be dangerous

Using WIFI connection are so fun. Do not try to do a transaction via WIFI. It could be you are being monitored by the bad guys , and your password could be stolen .

* Carefully when you take a promo on the internet

Do not easily tempted with the promo which was offered. Because when you give your credit card personal identity. Then it only was a fake. Your credit card will be cracked by someone with no responsibility