When precautions against possible problems, get yourself a

Business, Management

When your websiteappears vulnerabilities, hackers will easily attack the system, even controlthe management and cause bad consequences affecting the company’s reputation. Therefore, website security is one of the requirements to force, decide thesurvival of the site as well as the reputation for business. While it’s notpossible to remove 100% of cybercriminals, you can still protect your site withthe following 9 privacy rules. 1. Secure WebsiteWith Strong PasswordThis rule sounds prettysimple, but it is a very effective solution to help secure your website againstexternal sabotage.

Imagine this The thief will not be able to break into yourhouse if the wall is high, with barbed wire around it. Setting the password forthe site is similar. A strong password will prevent many hacker intrusions. To be called strong, your password should meet the following requirements – Password must be eight characters ormore – Password should include letters, numbers, special characters (e. g.

, @, #, $,%, ..) – In the password should be at leastone capital letter and begin with special characters – Different accounts need to usedifferent passwordsRemember ensure thesecurity of the website; you should change the password regularly, preferablyperiodically about once a month. 2. Update Regularly Technology is constantly developing, andhackers are also constantly upgrading themselves to be able to break intosuccessful websites through vulnerabilities.

Therefore, to increase the levelof security, you need to regularly follow up on the latest releases and constantlyupdate your site. This should be appliedto both the server operating system and other software running on your

website. Regular updates of bug fixes will help reduce the risk of hacking, data theft, administrator privileges, and so on. 3. Create The HabitOf Backing Up Important Data Hackers always make the site manager surprisewith the visit without notice. You will never know when hackers will come toyour site and also what he will steal. Therefore, to take precautions againstpossible problems, get yourself a habit of backing up important data right now.

This is also a way to secure the website effectively that any administratorshould do. This will help youovercome the consequences, restore the system faster and easier when theproblem occurs. At the same time, a recurring copy will be very useful when itcomes to resolving unexpected problems caused by a malicious server or website. 4. Increase TheSecurity Of The Server If you own a server system, it should be notedthat the machine configuration to ensure the maximum level of safety to theextent allowed.

To increase the security of your server, you need to do thefollowing – Uninstall (remove) all the junk orunused software – Develop rational policies for groupsand users – Deactivate unnecessary services andmodules – For certain data and directories, access restrictions should be set. – Check regularly for suspiciousactivities on the website – Use encryption and secure protocolsto better protect your server system5. Check For MalwareRegularly Currently, there are many types of securitysoftware to help ensure the safety of the site, but you should not besubjective, put on the life of your site for these types of software.

Everything goes wrong, including the best software. So, take a proactive scanof malware even everything seems to work normally. This test should beconducted periodically to ensure effective website and computer security.

6. Improve TheKnowledge Of Website Security As emphasized from the beginning, there are nosolutions that can guarantee your website 100% not attacked. Computertechnology is constantly changing and hackers, too, hacking techniques of hackersincreasingly sophisticated. Therefore, to best protect your website, networkadministrators need to constantly learn, improve their security knowledge, andregularly update new knowledge to respond to threats. From outside on time, avoid making mistakes, improve knowledge on website security7. ComputerSecurity Many malicious code attacks on the website aredistributed through the computer. Therefore, the security of the computer is avery important issue affecting the effectiveness of website security.

Keep yourcomputer safe with updated antivirus software. 8. Use The Security Tools WebsiteThere are now some freeand cost-effective security tools to help administrators protect their websitebetter. They operate on the same principle as the commands that hackers use tobreak into your site. Some of the free tools available today include – Net sparker – Open Vas – Security Headers 9. Use SSL Certificate To Secure Website When registering the domain for the website, there will always be security vulnerabilities for hackers to take advantage ofattack. SSL is a great way to protect your website and your customers. SSL is a globaltechnology security standard.

It can create an encrypted link between thehosting system and the browser. SSL enhances the security of your website, allowing all data exchanged between servers and browsers to be secure. Bottom LineThe website is the faceof the company, showing prestige, brand value. If the security issue is notproperly considered, malicious code can spread on the website and stealinformation from customers such as email, credit card.

From this, it can beseen that website security is a very important factor for online businesses. Hope the above 9 security rules will help you protect your website better.