Business guide to digital security

.nz

FROM HERE WE
CAN GO ANYWHERE.

netsafe

November 2013 by .nz

The Internet can help to transform the fortunes of smaller companies, but it pays to be aware of the risks that digital opportunities bring.

It's clear that the more companies invest in using the internet, the more they benefit. It is also clear that our customers are heavily engaged online and it is where businesses are expected to be. A recent Deloitte survey of small Australian companies found those that had embraced the internet saw revenues rise by an average of $A350,000 (or 20%). As a result, these companies had more diverse revenue streams, improved growth prospects and more clients, the survey found.

To make the most of opportunities that 'being online' offers, companies need to be aware of unique risks to their digital security. **Password theft, fraud, email scams and phishing, website attacks, hacking and malicious software can all lead to major losses – money, data and ultimately customer loyalty.** However, by following the simple steps in this guide and setting up solid IT practises, you can ensure both your company's computer systems and reputation are more secure.

New Zealand's smaller businesses are strong on agility and resourcefulness, but can struggle to keep up with technological change. With the increasingly widespread use of digital devices such as smartphones and tablets in the workplace, having a solid digital security policy is vital.

If you don't think this applies to your business, think again. Internet fraud in its many guises topped $4.4 million last year in New Zealand alone, according to independent internet safety organisation, NetSafe. Malware – malicious software designed to harm a computer system – can infect any size of company from one-man-band to multinational corporation and even governments.

It's not all doom and gloom, however. Being online is where your customers are and therefore where your company's future lies. By choosing to educate yourself and provide a great, safe experience for your customers, you'll improve customer engagement, reduce costs and drive revenue.

The Risks

WHAT ARE THE RISKS TO YOUR BUSINESS?

1__Fraud

In its annual review of cyber incidents, NetSafe reported New Zealand companies had lost $4.4m as a result of digital fraud of some description. A total of 562 of the 3,317 reports submitted to Netscape involved a financial loss. The average loss has also doubled year on year to $7,854, and last year there were seven reported losses exceeding $100,000. More than three quarters of reports NetSafe received were online scams and fraud.

'It's well worth doing five minutes research on what other customers are saying about a company before handing over payment,' says NetSafe. More than 350 people reported losing money after buying online, many from Facebook groups and little-known websites here and overseas. There are several types of fraud perpetrated online:

Ransomware__ A form of malware that denies access to a computer system then demands money for the restriction to be lifted, affected three Kiwi companies in September 2013 alone. There have been media reports from Australia that suggest some companies have paid ransoms up to A$5,000 to retrieve their data. But NetSafe advises companies not to pay the demand and to report it immediately. You can submit a report of a cyber incident online at www.theorb.org.nz.

Invoice Fraud__ This is a scam where companies are simply invoiced for goods and services they have not ordered. Each year in the United States, businesses pay many millions of dollars against fake invoices. These range from invoices for unwanted business listings and office supplies to demands from made-up charities.

While many assume this affects large corporations the most, SMEs are often targeted and should have in place a system for matching invoices to goods and services before they are paid. Pay particular attention to vendors with names that look similar to existing suppliers.

Email Fraud__ These are scams that try to get you to disclose personal details – often bank accounts – in order to extract money. There are many variations of the idea. Some of the most widely seen are:

- Your bank, or perhaps software vendor, needs you to update your online password by return of email. The email may be sent from an address that includes your bank's name and contain the right logo. But look carefully and you'll notice they are not the correct address, often containing subtle spelling differences.
- You have come into money from a long-lost relative, overseas lottery, the Bill Gates Foundation and the like;
- The sender is owed money and needs a foreign (i.e. your) bank account to pay that into;
- The sender is penniless and needs a loan.

2__Viruses

A computer virus is a form of software that installs itself and then replicates in other computer programs, which are then considered "infected". Viruses perform mostly harmful functions such as spamming contacts stored in a system, draining storage space, corrupting data, accessing information, putting messages on screens and recording (or 'logging') users' keystrokes. Logged keystrokes can then be used to capture users' usernames and passwords to then gain access to accounts.

3__Hacking

Hackers can directly target a business by breaking into its system to get access to websites, servers, antivirus, email, social media, customer, financial and payroll accounts. Even the world's biggest names in software are not immune. In August 2013, a security researcher hacked the Facebook account of the social media giant's CEO Mark Zuckerberg's profile page. To combat this threat requires updating software with the 'fixes' that developers such as Apple and Microsoft issue on a regular basis.

Note that Windows XP users face a problem in 2014 when the system is to be retired as Microsoft will no longer be issuing these security updates.

HOW TO MANAGE THE RISKS?

NetSafe's guide for small businesses lists five ways to minimise digital risk:

1__Think before you click

As we have already touched on, emails can be big trouble if you don't know exactly who you are dealing with. So-called Phishing is an emailed form of social engineering attack that tries to elicit sensitive information from you. The emails are designed to look official so look at them carefully.

NetSafe advises that you:

– Learn about about the different phishing schemes;

– Be wary of emails requesting urgent account verification;

– Do not download and open attachments you aren't expecting;

– Avoid clicking on video and photo links posted on your newsfeed;

– Do not respond, download files or click on links to websites that you are wary of;

– Be wary of any 'too-good-to-be-true online offers; and

– Make sure your anti-virus software comes with anti-phishing tools. If it doesn't, look at installing the crowdsourced browser plug-in Web of Trust (WOT).

2__Update your software regularly

Software companies such as Microsoft and Apple issue regular updates to their products to plug loopholes. Updates should be made regularly to computers, servers, websites and antivirus systems as a minimum. Users who ignore these updates are putting their sensitive information at great risk.

The newest version of a software package is generally the safest. As NetSafe says, it’s also vital to check those applications that help view online content, read PDF files and play videos. The huge popularity of programs such as Adobe Flash, Java and Adobe Reader makes them an attractive target for criminals.

3__Backup files regularly

What would happen to your business if you lost all your data? That could include all customer and employee records, contracts and the software systems you use. Unless you backup your files regularly, that’s exactly the question you will be forced to answer. Many cloud systems, such as Google Drive back up files constantly, relieving the user of the task. But those stored on local hard drives need daily backing up.

NetSafe offers some useful back up tips:

- Plan for a worst-case scenario, no matter how unlikely that may seem (consider the Christchurch earthquakes)
- Backup all your data regularly and consider keeping multiple copies made over a period of time
- Encrypt or password protect your backups to ensure privacy
- Store your backups ‘offsite’ or in different locations to spread the risk
- Restore some data occasionally to ensure your backups work

4__Secure your wireless network

Without adequate protection, your wireless network may be free to use for anyone within reception range. In addition to using up your bandwidth and costing you money, those unauthorised uses could also access sensitive information. To do this you should:

- Make sure your encryption is up to the job. NetSafe says wireless modems or routers should use WPA2 encryption. If yours is WEP, change it.
- Use strong passwords (see point 5.)
- Change the router’s default login password.

5__Passwords

We use passwords for just about everything we do online, whether that's shopping, banking or simply using a phone or tablet. At least, we should do. But many of us set the simplest of passwords, if they bother at all, and rarely reset them. An easily guessed password is an invitation for hackers to access your information and devices.

Make sure you:

- Set a strong password. It should be a minimum of 15 characters long and contain a mix of numbers and letters in upper and lower cases. Make sure they are not predictable (e.g. "abcdefg12345678" If you feel you need a memorable name or phrase try substituting numbers for letters, like this: "A11bl4ck5w1n2oL1" (All Blacks win 2011).
- Keep it secret. The responsibility for an account comes back to its owner.
- Keep them unique. That means a different one for each device and account.
- Change them. Every three months rather than three years.
- If you write your passwords down, make sure you keep that place secret, too. Notes taped to the back of your laptop are not ideal.

Google shares some advice on passwords here. NetSafe also suggests looking at password management tools such as LastPass and KeePass.

Checklist

SECURE YOUR DIGITAL BUSINESS AND PROTECT YOUR CUSTOMERS.

○ Disaster recovery – have a plan for when things go wrong. Back up the system regularly and test that backups are working as they should.

○ Get good anti-virus software and update it regularly (viruses mutate).

○ Follow safe practices with portable media, such as USB memory sticks. It has been estimated that nearly a third of malware infections are spread in this way. You can configure your operating system to automatically scan or even refuse any USB stick.

○ Make sure your domain name is secure by hosting your website and email with reputable providers who maintain their systems. A good starting point is this list of domain name registrars. Also ensure that your registrant details are correct and that your UDAI is kept safe.

○ Secure your transactions by using SSL (Secure Sockets Layer – a technology that allows the sensitive information such as credit card numbers and login details to be transmitted securely) and use reputable transaction providers. If you need to learn more about SSL chat to your IT provider.

○ Train your staff. Staff need to understand why digital security is important and how to go about having it. This free handbook offers 10 great tips for your company.

○ Develop a cybersafe culture. With staff increasingly using their own smartphones, laptops and tablets for work, comes a bigger risk of importing malware into your company network. Even companies with small staff need policies that cover the dos and don'ts of working on a network. This NetSafe site offers great advice on how to draw up a policy and what to include in it.

○ Be wary of WiFi hotspots when travelling. If you travel for work, sooner or later you'll want to use a WiFi hotspot, such as those at airports and hotels. The trouble is, they are often unsecured, which means they could be camping grounds for hackers and malware. One way to minimise the risk is to use a Virtual Private Network, or VPN. These give you a secure Internet connection when you're accessing websites and also encrypt any data. Some VPNs are free, but even the paid ones aren't expensive and it's ultimately more cost effective than compromised data.

○ Review security regularly. Viruses mutate and new devices and software appear so quickly now that it pays to review all your security regularly.

○ If your company does not have a dedicated IT manager, appoint a person or team to do this or work with a professional IT partner.

○ Physical security. In case of theft, make it company policy that all devices – laptop, phone, tablet – need passwords to open them, which are changed regularly. If data held on the devices is commercially sensitive or considered secret, consider using full disc encryption or software to track, lock or even wipe clean your devices if they are lost or stolen.

○ Maintain your website. Treat your website system as something that needs updating as well as your software and passwords. This is especially true if the website's developer used a free tool, content management system or "ecommerce" platform. NetSafe says it has received recent reports of several company websites that had not patched underlying editing systems being hacked into.

If your customers are purchasing products and services online with you then:

○ Have terms and conditions that are easily understood and prominently displayed on your website. Ensure they cover all relevant legal points as well as roles and responsibilities.

○ Be accessible. Display your contact and location details prominently and make sure they stay up to date.

○ Clear privacy terms must be displayed, which commit your company to protecting data, and have a policy of doing this, too.

Reporting security incidents.

○ **www.theorb.org.nz** has been developed by Netsafe to offer all the New Zealanders a simple and secure way to report online incidents which may break NZ law or breach legislation.

Glossary

Backup Copying and archiving computer data – files, software – so it can be restored in the future.

eCommerce Electronic commerce, or more commonly e-commerce or eCommerce, is where products and services are sold over the Internet.

Hacking Bypassing a security system to access a computer system.

Malware Malicious software such as a virus designed to disrupt or damage a system.

Patch Software designed to fix bugs in a computer program or its data.

Phishing An email requesting verification of sensitive information such as bank account or credit card details. Emails often appear to be from legitimate sources.

Ransomware A form of malware that denies access to a computer system then demands money for the restriction to be lifted.

Social engineering A confidence trick to gather information, commit fraud, or gain access to a system.

Virus Self-replicating computer program that often perform harmful activity on a system.

About .nz and NetSafe

.nz is managed by .nz Registry Services (NZRS*), the wholesale provider of .nz domain names to a retail channel of registrars who offer .nz domain names to the public.

If you would like more information on our role and activities then please contact **info@getyourselfonline.co.nz**

If you would like more information about getting online with .nz then please visit **www.getyourselfonline.co.nz**

NZRS is wholly owned by InternetNZ (Internet New Zealand Inc.) which is the charitable open membership organisation dedicated to protecting and promoting the Internet in New Zealand. For more information about InternetNZ please visit **www.internetnz.net.nz**

The .nz domain name market is regulated by the Domain Name Commission Limited (DNCL). For more information about DNCL please visit **www.dnc.org.nz**

** New Zealand Domain Name Registry Services Ltd*

NetSafe is an independent non-profit organisation that promotes confident, safe, and responsible use of online technologies.

We promote cybersafety and champion digital citizenship by educating and supporting individuals, organisations and industry on a range of issues.

NetSafe is a multi-stakeholder partnership which represents a range of perspectives from New Zealand's cybersafety community.

For further information about NetSafe contact:
queries@netsafe.org.nz