directive

TECHMinutes

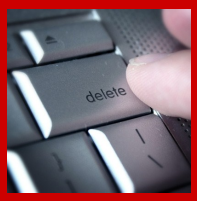
February 2012

Your Small Business Technology Information Source!

This Issue:

Data Capacity Soars

Hard drives have been getting



bigger (capacity-wise) and cheaper over the past decade which is great news for everyone. Toshiba predicts that in 2012 that over 2 zettabytes (2 trillion gigabytes!) of data will be created and replicated (double from 2010). While costs are going down, data growth is still a challenge for data centers and IT administrators.

Read the rest Online!
http://bit.ly/yg0oU3

About Directive

We are a technology consulting firm specializing in technology implementation and management for businesses. We're known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses.

Visit us **online** at:
newsletter.directive.com

Mobile Computing Cage Match

Busy business owners don't always have time to be technically savvy. Sure, you can pick things up pretty quickly, but when it comes down to the latest technology, you simply don't have the time to sit down and do the research. Walking down any electronics aisle you are likely to be bombarded by choices. Remember when it used to be simple? (Wait, it was never simple!) Let's classify some of the modern devices out there for mobility geared towards someone just like you.

Netbooks, Ultrabooks and Tablets Oh My!

If you want a portable device to take with you and get things done no matter where you are, you are in luck. The consumer electronics realm is flooded with great options to suite your need. The downfall? There are some bad eggs, and there are a ton of choices. Let's look at an old standard for our first contender.

The Laptop

These days, laptops, usually referred to as notebooks, don't carry the same commercial weight as some of the more modern devices. A notebook is a portable desktop, in a sense. Typically powerful, bulky, and not all that great on the battery life, this is the device you take from the office to your home, plug in, and keep tethered to the wall. They are pretty capable of replacing a desktop, and the more expensive ones are great for running more resource intensive applications like video editing and modern games. The pricing of notebook PCs vary greatly, from a few hundred dollars to a couple thousand.

Netbooks

Netbooks are essentially small notebook PCs. What does it take to be classified as a netbook? A screen smaller than 11 inches. They are very portable, have decent battery life, but they aren't very powerful. In fact, netbooks have received plenty of criticism, although they certainly do have their place. A typical netbook is cheap, usually substantially below the $500 mark, and travels very well. Many manufacturers have stopped producing netbooks although it's likely it will be a while before they are completely extinct. Honestly, if you just

(Continued on page 3)

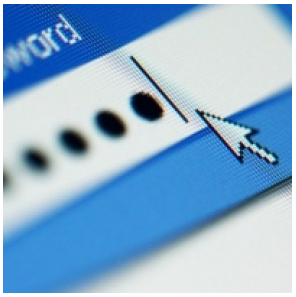
Disaster Recovery and Why it Matters

When you mention the term 'disaster recovery,' most people think about the big ground-shattering events like earthquakes, fires, floods, tropical storms, etc. While these natural events are certainly disasters and devastating in their own right, smaller things can constitute as a disaster for your business, and they aren't seasonal.
Let's look at the definition of disaster.

dis·as·ter

(Continued on page 4)

Facebook Logins Stolen by a Worm



On the topic of identity theft, social media accounts are becoming a high target for hackers, especially for spreading malicious viruses. To some, losing control over their Facebook or Twitter accounts could be just as devastating as having their credit card stolen. Trouble is, for many users, having one login account stolen means hackers have access to their other accounts too.

A piece of malware called Ramnit reportedly stole the usernames and passwords of over 45,000 Facebook users. It infects Windows applications and HTML files. A bulletin by security researchers at Seculert has been issued with the details of the malware. According to the bulletin, "Attackers behind Ramnit are using the stolen credentials to log-in victims' Facebook accounts and to transmit malicious links to their friends, thereby magnifying the malware's spread even further." The worm is capable of stealing other information as well, and has infected an estimated 800,000 machines since September. The majority of cases are from France and the United Kingdom.

Security is very important, and even if you are the type who wouldn't miss your Facebook account, the report adds, "In addition, cybercriminals are taking advantage of the fact that users tend to use the same password in various web-based services (Facebook, Gmail, Corporate SSL VPN, Outlook Web Access, etc.) to gain remote access to corporate networks." Keeping secure passwords and not re-using passwords across multiple networks is extremely important.

Directive suggests either coming up with your own password system for remembering multiple passwords across all of your accounts, or by using a secure password management system.

If hackers can get your credentials for Facebook, and you use the same credentials for your bank account, you may as well be leaving your keys, credit card, and wallet under the welcome mat for crooks. Employers will also want to educate their employees to prevent them from using the same passwords on company networks and accounts.

Share This Article!
http://bit.ly/y4LJFz

What to do when your Data is Breached

This has been a pretty common topic for us on the Directive blog. We've seen a lot of Upstate New York clients and customers suffer the consequences when online retailers and other account providers experience a security breach. It is equally vital for consumers to know what to do in the event of a security breach as it is the company that is actually breached.

Business Responsibility

Last week Zappos, a widely popular online shoe and clothing store, informed customers via email that its database had been hacked, and usernames and passwords have been stolen. Zappos, known for being a very modern, innovated business, reacted quickly and reset all passwords and quickly let all customers know about the breach.

This is an extremely important step for a business facing a large scale security breach. Letting your customers know that their data was stolen and that you are taking measures to resolve it can help maintain trust. Zappos is also being very transparent about what data was stolen. Think of it this way; if your credit card information gets stolen during a transaction, wouldn't you want to be informed about it quickly? Fortunately, no credit card info was stolen by the hackers in this case, but it is a very common circumstance in these types of events.

Customer Responsibility

If you a customer of a business that has experienced a security breach, you'll want to take action. Not all companies will be as responsible as Zappos and reset your password or immediately tell you what data was stolen. In this case, everybody's Zappos account is safe, but one major flaw in security needs to be considered for most users. It's pretty common for users to use the same password for multiple accounts. If a user has the same email and password credentials for both their Zappos account and their Facebook account, that means the hackers could get access to your Facebook.

If you use the same email account and password for multiple sites, you'll need to perform a password audit and create new passwords. Remember many online accounts can hold credit card and banking information, and you definitely don't want to have to deal with the repercussions of hackers getting into them. It is very important these days to keep track of all of your online accounts and utilize unique passwords for each account.

Share This Article!
http://bit.ly/x9OSVD

Mobile Computing Cage Match

(Continued from page 1)
want a cheap, reliable device that can do basic document editing and web surfing that isn't a hassle to lug around conferences and events, a netbook is the low-cost way to go.

Ultrabooks

Ultrabooks are the new thing (at least one of the new things). Ultrabooks are designed to be ultra-portable laptops. Think of them as a hybrid between notebooks and netbooks. Ultrabooks are actually defined by some standards put in place by Intel. They are typically less than an inch thick, weigh in less than 3.1 pounds, and have a good battery life of 5 to 8 hours. These razor-thin devices are fairly powerful and can load standard business apps quickly. Ultrabooks aren't quite desktop replacements but have significant power over a netbook without sacrificing portability and battery life. Think of the Ultrabook as a lightweight notebook.

Tablets

The tablet market is still fairly young but we're seeing a lot of great devices hit the market these days. Of course, the standards have been set by Apple's iPad, although several manufacturers are producing great Android tablets. One word of warning; you really get what you pay for with a tablet. If it is comparably cheaper than the iPad, it's quality is likely to be similarly less. The true test of a tablet is the apps available for it. Currently this puts the iPad on top, with Android quickly catching up. Later on this year Microsoft's Windows 8 operating system will start rolling out on tablets too, so we're likely to see some pretty interesting things over the next year. Don't think of a tablet as a replacement for your laptop/netbook/ultrabook unless you are willing to cope with the fact that it doesn't run all of the same applications. You can surf the web and edit documents (and even get separate keyboard peripherals for easier typing), and there are plenty of solutions to make a tablet very productive.

Looking for a mobile solution and need a little advice to determine what would work best for your needs? Contact Directive at 607.433.2200 and we'd be happy to discuss your needs.

Share this Article!
http://bit.ly/wndzyb

What is your Identity Worth to You?

Your identity has quite a lot of value, especially in the wrong hands. Security firm ZoneAlarm put together some numbers in 2011 concerning identity fraud, and it even shocked us. Let's talk about a few of these statistics and what it means.

First of all, what shocked us the most is that according to the FTC, in the United States, 9 million individuals have their identities stolen each year. Identity theft is a little different than identity fraud, however. Theft is when personal information is exposed and taken without permission. This is happening all the time by malicious software like spyware, but it can also happen when legitimate websites and services get infiltrated by cybercriminals. If a reputable online store (or even a database for a brick and mortar store) gets hacked into, your personal information can be stolen. That's identity theft.

Identity fraud is when that data is misused for financial gain. This is when things start to get very dangerous. In 2009, $56 billion dollars were accumulated by cyber criminals through identity fraud. The good news is in 2010 that number went down to "only" $37 billion. What does that mean to the average person? On average, victims of identity fraud had $4,841 dollars stolen per victim. Trouble is, the world has had to improve drastically to protect consumers from identity fraud. This means higher costs of doing business which then get reflected on prices of products and services. In other words, because of identity fraud, we all lose.

How does your data get stolen? There are plenty of ways, but here are a few popular methods:

1) Hackers can pick up credentials via public Wi-Fi and public PCs.
2) Credit Card Skimming - a process that involves your credit card data being stolen when your credit card is swiped at a standard ATM or credit card terminal.
3) Selling or discarding used computer equipment that isn't properly wiped can expose personal information.
4) Hackers can infiltrate networks and databases.
5) Dumpster diving and paper mail theft.
6) Malware and viruses
7) Phishing.

In almost half of reported identity theft cases, the victim knew the criminal.

(Continued on page 4)

Disaster Recovery and Why it Matters

(Continued from page 1)

A calamitous event, especially one occurring suddenly and causing great loss of life, damage, or hardship, as a flood, airplane crash, or business failure.

To Directive, a disaster is anything that involves a major loss of data or major downtime. When one of our clients experience a server malfunction that leaves most employees sitting idle unable to work, that is a disaster.

The Cost of a Disaster

Downtime is a very terrible expense to not try to avoid. Try this simple formula for yourself:

Number of Employees Affected by an IT Outage X Average Employee Hourly Cost (NOT WAGES)
+ Average Company Hourly Income X Percentage of Income Lost Due to the IT Outage

This simple formula will tell you about how expensive every hour of downtime is for your company. The hardest value in the formula is understanding the percentage of income lost. Not all companies might have a figure, but you will want to consider it as you do the math. This doesn't include the cost of repair, consultation, parts, or any of the remediation required to get things back up and running.

Disaster's Harbinger

Disaster can strike from any direction. Hard drives can go, data can be corrupted, hardware can fail, and networks can go down, and systems can become infected with … viruses and malware. User error can cause disaster, as well as theft and other malevolent activity. While companies should take precautions to safeguard themselves against threats both external and internal, and managed maintenance can prevent a lot of foreboding issues, having a solid disaster recovery starts with the data ….

Read More Online!
http://bit.ly/xGPORG

We partner with many types of businesses in the area, and strive to eliminate IT issues before they cause expensive downtime, so you can continue to drive your business forward. Our dedicated staff loves seeing our clients succeed. Your success is our success, and as you grow, we grow.

Chris Chase
Solutions Integrator

What is Your Identity Worth to You?

(Continued from page 3)

What do you do if your identity is stolen?

Almost half of all reports of identity frauds are discovered by the user first, although banks and credit card companies have methods in place to stay on top of it as well. If your financial credentials are stolen, you need to contact your bank and/or credit card companies immediately, both by phone and in writing.

You'll want to file a police report with details about where your identity was stolen, what you believe was or could have been stolen, and documented proof of the crime.
You don't want to risk identity fraud. Monitor your credit reports closely, shred sensitive mail and documents before throwing them away, and ensure your computers and network are running latest security updates and antivirus, as well as other security measures. For a complete review of your security, contact us at 607.433.2200 and we will help pinpoint vulnerabilities and fill in the cracks before a costly event occurs.

Share this Article!
http://bit.ly/AgCmAt

Charlotte Chase
Solutions Integrator

Directive

330 Pony Farm Road
Suite #3
Oneonta, NY 13820
Toll-Free 888-546-4384
Voice: 607-433-2200

Visit us **online** at:
newsletter.directive.com

facebook.directive.com
linkedin.directive.com
twitter.directive.com
blog.directive.com
newsletter@directive.com