

# MC Connect

*"Insider Tips to Make Your Business Run Faster, Easier, and More Profitably"*

## New Legal Reasons Why All Businesses Need An E-mail Archiving And Management System...

### It's a classic he-said, she-said case that ends up in court on a daily basis...

Widget buyer Ms. Robinson testified that Mr. Smith, the Widgets Corp. sales manager, told her that if she put her order in immediately, the price would be discounted by 20 percent. Mr. Smith argued that that was not what he said. According to his testimony, he agreed to give a 20 percent discount only if Ms. Robinson ordered at least one million widgets, which she did not. The widgets were manufactured and delivered, and the client was billed for the full amount. The client is refusing to pay the full amount and the manufacturing company is throwing it to a collection agency. If brought into a court of law, who would be right?

### Provided that neither party can produce a signed contract to back up their case, there is no way of knowing who is right.

However, let's suppose Ms. Robinson produces an e-mail she sent to her boss copying Mr. Smith that says, "I made a deal with Mr. Smith, the sales manager at Widgets Corp., to get a 10 percent discount for 500,000 widgets ordered." Let's also suppose Mr. Smith cannot produce any e-mails, contracts, or memos to the contrary. Now the chances of Ms. Robinson winning her case go up exponentially. When faced with two credible witnesses whose recollection of an event or agreement are in dispute, the court is most likely to favor the person who has corroborating documentation to support their side of the story.



"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

- Justin Shelley, Master Computing

February 2015

DENTON, TEXAS

### Inside This Issue...

New Legal Reasons Why All Businesses Need An E-mail Archiving And Management System...Page 1

Broken Hearts And Stolen Data...Page 3

How To Keep Your Laptop Secure When Using Public WiFi Hotspots...Page 4

How To Get 7 Years Out Of Your Laser Printer...Page 5

How To Grow Star Performers...Page 6

History Of Valentine's Day...Page 7

Protect Yourself From Online Credit Card Fraud...Page 8



"Sure, it's all fun and games until someone loses an iPhone."

---

## **E-mail has Become the Primary Means of Communication and Negotiation**

In the not too distant past, business people would communicate primarily through face-to-face meetings, telephone conversations, faxes, and the occasional paper document. When a "my word against your word" dispute arose, a court case could be awarded to the person who seemed more confident or credible.

Nowadays, e-mail has become the default mode of communication. It's very common for a buyer to communicate to a seller entirely by e-mail. Transactions are done without the two ever meeting and in some cases, never speaking. As a result, the "my word against your word" conundrum becomes more of a contest between e-mails, as opposed to a competition between the memories of the people involved.

The upside of this situation is that if you can produce an e-mail that supports your version of the facts, you have a leg up if it goes to court. The downside is that most people are careless about what they say in an e-mail. They don't think about it ending up as an exhibit in a courtroom under close scrutiny leaving them with the only explanation, "I know that's what I said, but that's not what I meant."

## **Food Service Company Awarded \$2.5 Million Thanks To A Few "Innocent" E-mails**

\*Example: A food service company was contracted to provide all meals at 48 nursing homes. Ultimately, the food service company claimed that it was underpaid over \$2 million and sued in federal court. The president of the nursing home company claimed that the food service company had made certain oral cost guarantees that were not honored, thereby justifying the underpayments. However, a detailed review of the nursing home company's internal e-mails revealed that its executives had "privately" expressed substantial doubt about the supposed oral guarantees. The e-mails were given to the jury, which awarded the food service company \$2.5 million.

## **What Should You Do To Protect Yourself?**

The most important thing you can do is think twice before hitting "send." If you are a manager or employer, train your employees to be careful about what they communicate via e-mail and constantly remind them of the dangers. Once an e-mail is sent, you cannot get it back. Another good practice is having a system for archiving and managing e-mail communications. This goes double for certain companies because of regulations like the Sarbanes-Oxley Act.

\*Story reprinted from How E-Mail Is Revolutionizing Litigation -- and What You Should Be Doing About It by Michael G. Trachtman, The Corporate Counselor, [www.law.com](http://www.law.com)

## Broken Hearts and Stolen Data

While many people buy their significant other a box of decadent chocolates, a dozen red roses or an oversize teddy bear for Valentine's Day, there are a few people who are going to go home with a broken heart as their personal information is stolen right from under them. It's a harsh reality, but both individuals and businesses are constantly targeted by fraudsters and hackers who want to steal any bit of data that will make them money.

You may have taken all the precautions to protect yourself and your business – but what do you do if it does happen? Just as when a lover breaks your heart, you have to move on, get back on your feet and work your way through this unfortunate circumstance.

Once your data is stolen, it's gone. Credit cards can be canceled, but other information, such as your name, address, social security number and more, can be more difficult to control.

In 2014, social media accounts, such as Twitter, became more valuable to hackers than credit cards. These types of accounts are hot commodities on black markets.

Does that mean you should be worried with all the information you have stored online? Absolutely not!

### If you do fall victim to a data breach, you can still protect yourself!

**Contact your credit card companies.** Let them know you suspect your credit card info has been compromised. They will work with you to ensure you don't face financial losses.

**Keep a close eye on all your accounts.** Watch for suspicious activity and report it when you see it.

**Change your passwords.** This is particularly critical if you used a single password for multiple services.

**Use a credit-monitoring service.** They aren't designed to prevent data from being stolen, but in the event of a breach, you'll be notified immediately so you can take action.

Give us a call at 940-220-7817 and we'll put together a plan to keep your company's data secure.

## How To Keep Your Laptop Secure When Using Public WiFi Hotspots

They are everywhere these days. WiFi hotspots for checking e-mail and hopping on the Internet can be found in airports, coffee shops and even most fast-food joints. But have you ever wondered, just how safe is it to connect? With the proliferation of hackers, viruses and identity theft at an all-time high, you are smart to be concerned. Unfortunately, it is easy for a hacker to set up a WiFi spot to access your laptop, called an “evil twin.” An evil twin is a wireless hotspot that is used to lure people from a nearby, legitimate hotspot. For example, when logging in at your favorite coffee shop, you may have inadvertently logged in to an evil twin Internet connection set up by the person working on a laptop at the next table.

Just like legitimate sites, evil twins allow you access to the Internet, but in the background they record everything you are typing. Log on to your e-mail, investment web site or bank account, or buy something online, and they are recording your keystrokes.

**Tip:** Do you want an easy way to securely access your network and the Internet from anywhere? Call us today at <your phone # here> about setting up a VPN for your office!

You may be asking, “How do I protect myself at WiFi hotspots?” First you need to make sure the hotspot is legitimate. You can do this by asking someone who works at the WiFi location; in fact, some businesses will give you printed instructions that include the hotspot name. Even here you need to be careful. Many times, in an attempt to make you feel comfortable, the hacker will use an evil twin name that mimics the legitimate hotspot and, on some occasions, the fake site may even show up at the top of your network list by having a stronger signal than the legitimate site.

### **The best protection you can have is connecting via your company’s VPN (virtual private network).**

A VPN protects your online information by encrypting your data and activity even if you're connected through an evil twin. If you don't have a VPN, the best protection is to surf the net, but never type in password, credit card, social security, bank account or other sensitive information when connected to a public WiFi hotspot.

## **Shiny New Gadget Of The Month:**



### **Prizm**

This month's gadget is so new, it isn't even off the assembly line. Meet Prizm — a small, pyramid-shaped device designed to make your home-audio experience as hands-off as humanly possible. The device was recently backed on Kickstarter this past November. The French company behind the audio device wanted to create an intuitive music experience that brings users new music, while learning what they really love to listen to.

The device streams music from cloud services such as Deezer, Spotify and SoundCloud, with more services planned in the future. It works by accessing your WiFi network. It doesn't contain any speakers, so you'll have to supply your own (it connects via Bluetooth, 3.5 mm stereo jack and optical audio). And despite being called hands-off, the device sports buttons to let you like or skip songs to customize your listening experience.

It can currently be pre-ordered from [www.meetprizm.com](http://www.meetprizm.com) for \$139.

## 3 Easy Steps To Get 7 Years Of Hassle-Free Service Out Of Your Laser Printer

Printers - the necessary evil of every office. From paper jams and error messages, to problems like smearing, misfeeds, and ghosting, printers can really make your blood pressure rise.

Plus, it's easy to sink thousands of dollars into maintenance and repairs. If you want to avoid common printer problems AND save yourself a small fortune on replacements and repairs, follow these 3 easy steps:

### Keep It Clean

There is no faster way to gunk up a laser printer and cause printing problems than by letting it get dirty.

On a monthly basis, use compressed air to blow out the inside of the printer. Remove the toner cartridge for better access, and don't forget to do the back if it is accessible. It also helps to take a vacuum to the outside. If you print labels or use any other type of specialty media like transparencies, use rubbing alcohol to clean the rollers inside the printer.

### Do Your Maintenance

You can almost infinitely extend your printers lifespan by doing the regular maintenance suggested by the manufacturer.

This includes replacing rollers, filters, and occasionally replacing the fuser (the printer's internal furnace.) Here's a little money-saving secret: you only need to do this type of maintenance at 1.5 to 2 times the manufacturer's usage recommendation. In other words, if your printer's manufacturer says to replace rollers every 100,000 pages, you really only need to do so every 150,000 to 200,000 pages.

### Use a Surge Protector

Nothing will send your printer to the bone yard faster than an electrical surge caused by lightning or other issues on the power grid.

When internal components are fried, it is often cheaper to buy a new printer than it is to fix the existing one. It is easy to protect yourself with a \$25 surge protector. DO NOT plug a laser printer into a UPS or other battery backup system. The printer's power draw is too much for a battery to handle.

## HOW TO GROW STAR PERFORMERS

A study of computer programmers at Bell Laboratories showed that the star performers outperformed moderate performers by a margin of 8 to 1. If that holds true in your organization, the conversion of five of your moderate performers into star performers would be the equivalent of adding 35 moderate performers to your workforce. Where are you going to find the five additional star performers? You don't find them. You develop them.

The Bell Labs study identified nine work strategies that characterize star performers. All of them are qualities that can be inculcated through a good corporate education system. According to researchers Robert Kelly and Janet Caplan, these qualities are:

- 1) **Taking initiative:** accepting responsibility above and beyond your stated job, volunteering for additional activities and promoting new ideas.
- 2) **Networking:** getting direct and immediate access to coworkers with technical expertise and sharing your own knowledge with those who need it.
- 3) **Self-management:** regulating your own work commitments, time, performance level and career growth.
- 4) **Teamwork effectiveness:** assuming joint responsibility for work activities, coordinating efforts and accomplishing shared goals with workers.
- 5) **Leadership:** formulating, stating and building consensus on common goals and working to accomplish them.
- 6) **Followership:** helping the leader to accomplish the organization's goals and thinking for yourself rather than relying solely on managerial direction.
- 7) **Perspective:** seeing your job in its larger context and taking on other viewpoints, like those of the

customer, manager and work team.

- 8) **Show-and-tell:** presenting your ideas persuasively in written or oral form.
- 9) **Organizational savvy:** navigating the competing interests in an organization, be they individual or group, to promote cooperation, address conflicts and get things done.

Star performers considered initiative, technical competence and other cognitive abilities to be core competencies. Show-and-tell and organizational savvy were on the outer edge of their circle of importance. Middle performers placed show-and-tell and organizational savvy at the center. While star performers were focused on performance, middle performers were focused on impressing management.

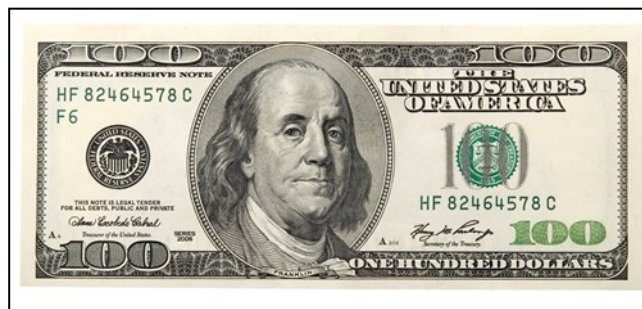
Star performers and middle performers also showed marked differences in their attitudes toward networking. The middle performers waited until after they had encountered problems before looking around for someone who could provide help and support. The star performers built a network of helpers and supporters in advance, so they could call on them immediately when needed.

The study concluded that "Individual productivity... depends on the ability to channel one's expertise, creativity and insight into working with other professionals."

Star performers emerge from educational systems tailored to the individual company and the individual job. They don't want to become clones. Too many companies today are content with training programs that provide people with knowledge and expertise, but skimp on educational processes that teach them to apply what they learn. You can't train them to seek excellence. You change that attitude through consistent input that appeals to an individual's self-interest and organizational spirit.

## Refer Our Services And We'll Donate \$100 To Your Favorite Charity!

We love having you as a customer and, quite honestly, wish we had more like you! So instead of just wishing, we've decided to enact a new "refer a friend" policy. Refer any company with 10 or more computers to our office to receive a FREE Computer Network Assessment (a \$397 value). Once we've completed our initial appointment with your referral, we'll donate \$100 to your favorite charity (even if that favorite charity is you) for every referral that you've sent, as a small thank-you for thinking of us.



Simply call us at 940-220-7817 or e-mail us at [connect@master-computing.com](mailto:connect@master-computing.com) with your referral's name and contact information today!

Master-Computing.com  
[connect@master-computing.com](mailto:connect@master-computing.com)  
 940-220-7817

**MASTER**  
 COMPUTING

## The History of Valentine's Day

By Jessica Shelley



What is Valentine's Day? There isn't a lot known about Saint Valentine. In fact, there are at least three Saints recognized by the Catholic Church named Valentine or Valentinus. What we do know, however, is that February has been a month of romance since before the Middle Ages.

Much like Christmas, Valentine's Day was used to replace a Pagan celebration called Lupercalia by the Catholic Church. This fertility festival was dedicated to Faunus the Roman god of agriculture as well as the Roman founders Romulus and Remus. During the festival, members of the Luperci, an order of Roman priests, would gather and sacrifice a goat, for fertility, and a dog, for purification. After the sacrifices had been completed they would then strip the goat's hide into strips, dip them in sacrificial blood, and take them to the streets where they would gently slap both women and crop fields in order to promote fertility and growth.

Many Romans believed that February 14<sup>th</sup> was the beginning of birds mating season which added to February 14<sup>th</sup> being a day of romance. People began exchanging cards in the 16<sup>th</sup> century.

The oldest Valentine's Card that is still in existence was a poem written in 1415 by Charles, Duke of Orleans, to his wife while he was imprisoned in the Tower of London. Towards the end of the 17<sup>th</sup> century the exchanging of gifts and notes as a way to express love became very popular. Today, Valentine's Day is the second largest card-selling holiday of the year, right behind Christmas.

So, don't forget to remember your loved ones this Valentine's Day and continue this ancient tradition.

## Protect Yourself From Online Credit Card Fraud



The past couple of years have been a rough ride for anyone who relies on a credit card to make purchases. Data breaches have plagued retail stores in the U.S. and Canada. Credit card providers are set to roll out new, more secure credit cards to consumers this year, catching up to Europe and

much of Asia in terms of credit card security. The U.S., in particular, has lagged behind in credit card security due in part to the cost of upgrading both the cards themselves and the pay terminals.

If you are concerned about your credit card information falling into the wrong hands, there are several steps you can take to protect yourself:

**Only give your credit card information to secure and trusted web sites.** Never enter any personal or financial information on a non-secure web page. If you don't see "https" in the web address, move along.

**Monitor all activity.** Regularly check your credit card and bank statements. The simplest way to spot fraud is to monitor all your financial activity. Many credit card providers have custom alerts you can set to notify you if certain purchases are made.

**Never save credit card information.** Many online retailers and shops now ask if you would like to save your credit card information for future use. While it may seem convenient, skip it.

**Delete your cookies and auto-fill data.** When you enter information on a web page, that data is stored in your web browser. After you complete a transaction, go into your browser's options, settings or history tab and delete the data.

## How To Pick A Good Password

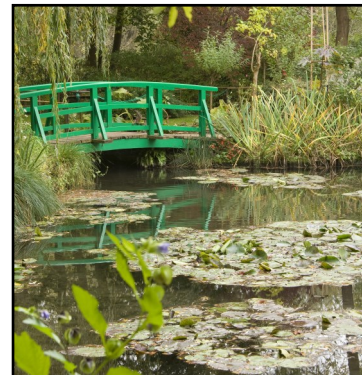
What's the most common password? You guessed it..."password." Obviously this is not the best way to protect yourself against hackers and online thieves. But even if you don't use the word "password," you might be using an equally easy password to decipher.

We suggest you DON'T use the following passwords for really important web sites, such as your online banking web site or other financially related sites.

- Your name or your spouse's name.
- Your children's names.
- Your pet's name.
- Your birth date.
- The last four digits of your Social Security number.
- Your phone number.
- Your address.
- A series of consecutive numbers, such as "1, 2, 3, 4."
- A single word that would appear in a dictionary.

Your best bet for creating a strong password: Use combinations of letters, numbers and special characters.

## The Lighter Side: Punch a Painting, Go to Jail



In 2012, Andrew Shannon punched a Monet painting valued at \$10 million. The incident occurred at the National Gallery of Ireland, located in Dublin. The painting, entitled *Argenteuil Basin with a Single Sailboat*, painted in 1874, apparently represented something much greater to the man who decided to attack it.

Right after his initial arrest, Shannon said the attack represented his way of "getting back at the state." Later on, when he appeared in court, he changed his tune. Instead of an "attack against the state," he said the whole thing was just a big misunderstanding. He said he didn't punch the painting, he "fell into it." He told the court he had felt faint and fell. The painting just happened to be in his way.

Fortunately, the National Gallery has plenty of CCTV cameras and the whole thing was recorded. What did those cameras see? Andrew Shannon very deliberately thrusting his fist through the Monet painting. In December of 2014, he was sentenced to five years in prison, and *Argenteuil Basin with a Single Sailboat* is back on display after being fully restored.