



The 5 Most Dangerous Pieces Of Information To Give In An E-mail

In the book *Spam Nation*, investigative journalist and cybersecurity expert Brian Krebs revealed the single most effective (and relied upon) way cybercrime rings gain access to your bank account, credit cards and identity. Ready for it? E-mail.

Whether it's opening an attachment infected by a virus, or a phishing scam where you unknowingly give up your login to a critical web site, e-mail still remains the most popular and reliable way digital thieves can rob you blind, steal your identity and wreak havoc on your network. Worst of all? You're INVITING them in! While there are a number of things you need to do to protect yourself, here are five pieces of information you (and your team) should NEVER put in an e-mail.

1. **Your social security number.** Think of this as your "bank account" number with the government. You should never e-mail this to anyone because it can be used to open credit cards and steal your identity.
2. **Banking information.** Your bank account numbers, routing number and online banking login credentials should never be e-mailed. Further, avoid sending a voided, blank check as an attachment to an e-mail.
3. **Your credit and/or debit card information.** NEVER update a credit card via an e-mail! If you need to update a card with a vendor, there are two safe ways to do this. The first is to log in to your vendor's secured site by going to the URL and logging in. Do NOT click on a link in an e-mail to go to any web site to update your account password or credit card! Hackers are masters at creating VERY legit-looking e-mails designed to fool you into logging in to their spoof site, which LOOKS very similar to a trusted web site, to enter your username, password and other financial details, thereby gaining access. Another way to update your account is to simply CALL the vendor direct.
4. **Login credentials and passwords.** You should never share your passwords or answers to security questions with anyone for any site, period.
5. **Financial documents.** An ATTACHMENT that includes any of the above is just as dangerous to e-mail as typing it in. Never e-mail any type of financial documents (or scans of documents) to your CPA, financial advisor, bank, etc.

Remember: Banks, credit card companies and the government will never ask you to click a link to provide them with any of the five items above. If you get an e-mail requesting you to update any of the above information, there's a good chance it's a phishing e-mail from a hacker. Don't be fooled!



"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!"
- Shawn Butt
Zaphyr Technologies

June 2015

Whippany, NJ

Inside This Issue...

The 5 Most dangerous Pieces of Information to Give In An Email...Page 1

How To Make Yourself 'Invisible' To Hackers...Page 2

We Love Introductions ...Page 2

InfiniteUSB...Page 3

4 Ways to get More Performance, Productivity and Profits...Page 3

How To Know When An Employee Is About To Quit...Page 4

Lost In Translation: Advertising Blunders...Page 4



How To Make Yourself 'Invisible' To Hackers

There's an old joke about two men hiking in the woods when they come across a big, grumpy black bear. Scared silly, one of the guys starts to run but notices his buddy stopped, bent-over, changing his shoes. He shouts to him, "Dude! What are you doing?!?! Why aren't you running?" to which his friend replies, "I'm changing my shoes because I don't need to outrun the bear - I only need to outrun YOU."

This is a perfect analogy for what's going on in small businesses: the "slow," easy targets are getting nailed by fast-growing cybercrime rings that are getting more sophisticated and aggressive in attacking small businesses. Last year, the average cyber-attack cost a small business \$20,752, a substantial increase from 2013, when the average was \$8,699. That's because most small businesses don't have the security protocols in place or the manpower and budget to implement sophisticated security systems. While there's absolutely no way to completely protect yourself other than disconnecting entirely from the Internet, there are several things you can do to avoid being easy pickings. Here's how:

1. **Lock your network.** While WIRED networks make you invisible to WiFi snoops because you have to access them by plugging into physical outlets or hacking modem ports, you can create a hidden or cloaked network on a wireless network. Simply disable the service set identifier (SSID) broadcasting function on the wireless router, and only users with the exact network name will have access. Small businesses like coffeehouses can also do this — just periodically change the network's information and place a small sign near the register with the current network name and passcode.
2. **Encrypt your data.** On your desktops, turn on the full-disk encryption tools that come standard on most operating systems: BitLocker on Windows-based PCs and FileVault on Macs. There is no noticeable performance lag; however, the encryption only applies when users are logged out of the system. So setting computers to automatically log out after 15 minutes without use is a good idea. And for mobile devices, use a VPN (virtual private network) to encrypt data traveling to and from your mobile devices and limit your employees' access to only the company data that they must have to do their jobs.
3. **Install firewall and anti-malware applications** on all of your equipment, including mobile devices.
4. **Disable features that automatically connect your mobile devices to any available network.**
5. **Disable printer and file-sharing options on mobile devices before connecting to a hotspot.**
6. **Check before connecting to hotspots.** If there is an unusual variation in the logo or name on the login page, beware...this could mean it's a fake hotspot designed to steal your data.

Can you guarantee that the person across the hotel lobby isn't looking at your data? Not really, but the chances of them being able to do that are greatly reduced if you take precautions to protect your business.

We Love Introductions!



For any company that you introduce to us, we will give you a \$100 that you can use for yourself or donate to your favorite charity. If they become a client we will send you an additional \$100 check!

If you know someone that is looking for IT support contact us by:

➤ Calling us at 973-560-9050

OR

➤ Emailing us at Newsletter@Zaphyr.net

Shiny New Gadget Of The Month:



InfiniteUSB

As laptops grow thinner, USB ports become scarcer. This means that if you need to connect to many printers, phones, or a mouse, you need to carry around a multiport hub to plug in various devices. But Jiange has created a USB plug that is based on a daisy chain, allowing you to plug multiple devices into one USB port. It recently launched its product via a very successful Kickstarter campaign.

The design won an IF Concept Award from one of the most prestigious design competitions in the world. Jiange has a lot more design inventions underway. InfiniteUSB cables start at \$10, and will also come in varieties that support microUSB and Lightning connectors.

<http://getinfiniteusb.com/>

Four Ways To Get More Performance, Productivity And Profit From Your Team

1. Your Team Needs To Learn Together

Rarely do teams learn together. Too often, increases in skill are confined to individuals. Sometimes that can become a barrier to teamwork: because there are dramatically different knowledge and skill levels, some team members aren't able to keep up. When an individual attends a course or discovers a useful practice, he or she should be encouraged to share it with the team. And periodically putting the entire team into a learning environment is critical.

2. Peer Recognition Is Powerful

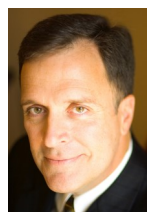
If you're a team leader, understand that despite your best efforts, you will be incapable of adequately recognizing every team member's efforts and contributions. Good work will slip by and go unrecognized. If this happens often, the team member may well become disillusioned. Relieve yourself of the burden to be the sole dispenser of recognition: ask team members to recognize each other. Make it a team expectation to thank other team members for their assistance and to look for opportunities to catch each other doing something praiseworthy.

3. To Win More Together, Think Together More

Have you ever held a team retreat? When was the last time your team came together for the express purpose of thinking about the work you do? Do you periodically pause as a group to reflect on what you've learned and internalize the lessons? Do you meet to consider opportunities, and not just to solve problems? The team that thinks more wins more.

4. You've Got To Expect It And Not Tolerate It If You Don't Get It

Some managers, knowing how difficult it can be to create great teamwork, undermine their efforts by making teamwork "optional." That is, they appreciate the people who are good team players but they tolerate those who aren't. As the old adage goes, what you allow, you condone. Those on the same team should know that figuring out how to get along and work with other teammates is their responsibility. Those who refuse to be team players should at the very least not enjoy the same benefits, and at worst, should be removed. It might sound harsh, but it is necessary if you want teamwork to work.



Mark Sanborn, CSP, CPAE, is president of Sanborn & Associates, Inc., an idea studio dedicated to developing leaders in business and in life. Mark is an international best-selling author and noted authority on leadership, team-building, customer service and change. Mark is the author of 8 books, including the best seller *The Fred Factor: How Passion in Your Work and Life Can Turn the Ordinary into the Extraordinary*, which has sold more than 1.6 million copies internationally. Learn more about Mark at www.marksanborn.com.

How To Know When An Employee Is About To Quit

There's nothing quite as devastating as losing a key employee, especially if they give you no warning or notice. Often they'll give you subtle signs such as a lackadaisical approach to work, arriving and leaving on time, not a minute sooner or later, long lunches or suddenly having several appointments at the beginning or the end of the workday. But one of the biggest giveaways is their Internet behavior at work.

We already know that employees spend personal time at work on Facebook and other social media sites; but you know something's going on if they've added monster.com, Craigslist, LinkedIn and other local job sites to the web pages they frequently visit.

That's ONE of the reasons we recommend our clients install an Internet monitoring software for their network. Not only will it reveal when employees are looking for work somewhere else, it will also alert you to employees who are wasting HOURS on social media, gambling, shopping and other non-work-related web sites. It will also prevent employees from accessing porn and file-sharing sites that could bring on a BIG lawsuit or nasty hacker attack.

While some people fear this is too invasive, keep in mind that you are paying those employees to perform a job with company-owned devices and company-paid Internet. We're not suggesting you monitor their personal devices or what they do after hours on their own time. But it's perfectly reasonable to expect an employee to put in a full 8 hours if you're paying them for their time.

Of course, you should provide notice that their computers are being monitored and set the expectation that you want them working during company hours; you should also detail what employees can and cannot do with company-owned devices in your Acceptable Use Policy (AUP). If you want to give them the ability to check personal e-mail and social media sites during work hours, you can limit it to 30 minutes a day during their lunch hour or break. Again, we don't recommend this since this can be an easy gateway for viruses and hackers—but these options are available.

Need help designing an employee monitoring system on your network? Give us a call. We can help you put together an Acceptable Use Policy and put the right software in place to enforce your policy.

Who Else Wants To Win A \$25 Gift Card?

Last month's Trivia question was **What is a petaflop? a) your dog after a long walk b) the latest toy for kids c) a measure of a computer's processing speed expressed as: a quadrillion (thousand trillion) floating point operations per second (FLOPS)**

The correct answer was **c)**. Now, here's this month's trivia question. The winner will receive a \$25 Amazon gift card.

June was named after the Roman goddess Juno. She was the goddess of what? a) marriage and childbirth b) fruit and trees c) religion d) love and beauty

* The winner can choose to have *\$25 donated in there name to a local charity of their choosing.

Call us right now with your answer!
973-560-9050

The Lighter Side: Lost In Translation: Advertising Blunders



- Clairol introduced a new curling iron they called the "Mist Stick" to the German market, only to find out that "mist" is slang for manure in German. Not too many people had use for the "manure stick."
- When Gerber started selling baby food in Africa, they used the same packaging as in the US that featured the "Gerber baby" on the front. Later they learned that in Africa, companies put pictures of what's inside the package on the label since most people can't read, thereby causing African consumers to think there was pureed baby inside.
- Colgate introduced a toothpaste in France called "Cue," the name of a notorious porno magazine.
- Pepsi's "Come alive with the Pepsi Generation" translated into "Pepsi brings your ancestors back from the grave," in Chinese.
- The Coca-Cola name in China was first read as "Ke-kou-ke-la," meaning "Bite the wax tadpole" or "female horse stuffed with wax," depending on the dialect. Coke then researched 40,000 characters to find the phonetic equivalent "ko-kou-ko-le," translating into "happiness in the mouth."