



Ribb"IT" Review

“Insider Tips To Make Your Business Run Faster, Easier, And More Profitably”

Issue 5 Volume 6 May 2013



“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!”
- Alex Bleam, Frogworks

Inside This Issue...

What It Takes To Win: Holding Nothing Back Page 1

Are You Still Using Outdated Tape Backups? Page 2

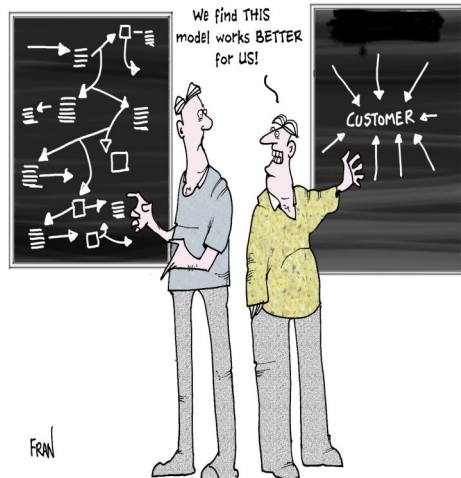
3 Things You Need To Know About E-mail Marketing Before You Press “Send” Page 2

Can Macs Get Viruses? Page 3

The Lighter Side: Philosophy Of Spring Cleaning Page 4

Dropbox: Is It Secure For Your Business? Page 4

Shiny New Gadget Of The Month: Intel Ultrabook Convertible Page 4



What It Takes To Win: Holding Nothing Back By Jennifer Bleam

Last month, I had the opportunity to meet Mike Ditka.

Many of the lessons learned on the football field can be applied to business and life.

Here’s a quick overview on what he shared about getting the right people on your team. He said, “The most important thing I did when I started out as a coach was to have good people around me, the right assistants.

And we had to discern who could stay, who could play, and who had to leave.” You have to have the right people in the right places if you’re going to succeed.

As you hire staff make sure they’re an ACE. (And evaluate yourself to make sure you’re an ace too!)

A - Attitude. There are many things you cannot control. But every day when you wake up, you CAN control your Attitude. You make choices that determine your attitude in life.

C - Character: Character is the fabric of your being, what you would die for. “If you have a good one, you have a chance.”

E - Enthusiasm: If you’re doing something, get excited about it. Get pumped up!

“You can’t motivate people. They gotta motivate themselves.”

Towards the end of our time together, Coach was asked, “How do you motivate people?” I think you’ll love his answer, “You can’t motivate people. They gotta motivate themselves... I like people who are self motivated.”

So, as you’re growing your company, make sure YOU are an ACE. Train your support staff to be a team of ACEs. Find out early (maybe even in the interview process) who is self-motivated and who is not. And then run for a touchdown!



Coach Mike Ditka agrees to sing “Hail To The Redskins” for Alex & Jennifer Bleam, owners, Frogworks.

Are You STILL Using Outdated Tape Backups?

If your computer network and the data it holds got erased or corrupted because of a virus, hard drive crash, fire, flood or some other random, unforeseen disaster, **how confident are you RIGHT NOW that your business could be back up and running again FAST?**

If your answer to that is, “I don’t know,” or “I’m not sure,” you are taking a HUGE risk with your company’s most important asset—the data on your network. Just imagine what would happen to your business if you lost your entire client database...

...Lost all accounting documentation and history...Lost all the work files you’ve spent YEARS developing...
Lost the work files and documentation you so desperately need to service your customers...

Can you even put a price tag on it?

Probably not—yet so many business owners aren’t 100% certain that they could be back up and running after a disaster and are purely *hoping* that their current tape drive or backup is working and storing a usable copy of their data.

Tape Drives Are The MOST Unreliable, Unsecured Way To Back Up Your Data

All tape drives fail; it’s only a matter of “when,” not “if.” So if being able to get back up and running again in the event of a data-erasing disaster is important, then you need to know about our Frogworks Sentinel

- ✓ You’ll eliminate expensive repairs and recovery costs.
- ✓ You’ll sleep easier knowing the “gremlins at the gate” are being watched and kept out of your network.
- ✓ You’ll safeguard your data.
- ✓ You’ll gain incredible peace of mind.

Want to know if your data is REALLY secure and being backed up properly? Call us for a **FREE** Data Backup and Disaster Recovery Audit. Call us at 240-880-1944

3 Things You Need To Know About E-mail Marketing Before You Press “Send”

It’s everyone’s favorite application. Since its introduction, it has revolutionized the way we communicate, both personally and professionally. It has had a major impact on how companies market themselves, communicate with vendors, send out press releases, rally employees and alert clients to their latest and greatest promotion. The ease, low-cost and speed of e-mail in marketing is the biggest reason why our inboxes are overflowing with spam.



In response to the ubiquitous outcry “I hate spam,” governments have crafted regulations surrounding the use of e-mail; and if you are one of the millions of companies using e-mail for marketing, then it’s important that you familiarize yourself with these laws. But the danger doesn’t stop there...

Even if you don’t get caught by the feds for violating the rules of e-mail usage, you can still end up on a blacklist with the major ISPs such as Yahoo!, Gmail, GoDaddy and Earthlink. Once you get blacklisted, you are considered guilty until proven innocent, and ALL the e-mail you send won’t get through, even to people who want to receive it—a consequence that could end up hurting your business more than a fine.

What Are The Basic Guidelines Of E-mail Marketing?

First and foremost, make sure you are only sending e-mail campaigns to people who have solicited (requested) to be on your distribution list. This is called “opting-in” or subscribing, and e-mails sent to these folks are considered “solicited e-mail.” You are perfectly within your rights to send them messages; but if you got their e-mail address by any other means and they did NOT specifically request to be on your list, that’s considered “unsolicited e-mail” or spam. Sending promotional e-mails to people who have not requested them is not only illegal, but annoying...so don’t do it!

Next, make sure you provide directions on how a person can remove themselves from your distribution list in EVERY e-mail. The best place to put this information is at the very bottom of your message. You should also include your full company name and contact information at the bottom so no one can blame you for cloaking your identity—another legal “no-no” of e-mail marketing.

Our #1 Recommendation

Lastly, when sending e-mail out to your marketing list, we recommend using a service such as Constant Contact or MailChimp. These web-based applications will help you manage your e-mail distribution list with automatic opt-out and opt-in tools and will keep your e-mail server off an ISP’s blacklist.

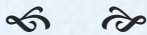
Naturally, you want to make sure the information you are sending is interesting and relevant. No one wants more junk filling up their inbox, so the better you are at marketing, the better your results will be. E-mail is not a magic marketing bullet that will solve all your marketing problems, but used correctly, it can certainly help you reach more customers and build stronger relationships with the people you already do business with.

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

The Grand Prize Winner of last month's Trivia Challenge Quiz is **Judy Speaks at Heidler, Inc. Heidler, Inc is an award winning plumbing and heating contractor in Annapolis, MD.**

Judy was chosen at random among those entries with the correct answer to my quiz question from last month: April is named after the Greek goddess, Aphrodite. She is the goddess of?

The correct answer was c) Love.



Now, here's this month's trivia question. The winner will receive a \$25 gift card to **Red Lobster.**

Which May celebration was first observed in 1908?

a) Kentucky Derby b) Mother's Day c) Cinco De Mayo d) Memorial Day

Email our marketing manager: Jennifer@GetFrogworks.com with the word "Trivia" in the subject. Or call us right now with your answer! 240-880-1944

All correct answers will go into a drawing which will take place on the 15th of the month. Good Luck!



Can Macs Get Viruses?

A very common misconception is that Apple Mac products cannot get viruses. Not true! There is no such thing as a 100% safe computer. Devices running OS X, Windows, Linux, Android or any other operating system are all capable of being infected with a virus or other malware.



However, the likelihood of an Apple Macintosh user gets a virus is much lower than for Windows users. In fact, many Apple users don't even run any antivirus software on their computers. Whether that is a smart strategy is debated by many IT professionals.

A few of the reasons why Macs don't get as many viruses as PCs are:

1. Mac OS X is based on the Unix operating system, which is one of the oldest and most secure operating systems around.
2. Microsoft Windows is used by many more people, so it's a bigger and better target. Plus the way that Windows is built makes it easier for viruses to spread across computer networks.
3. Many of the tools designed to create viruses or malware are written for the Windows operating system.

Windows Threats Even For Macs

Many Mac users find themselves having to use Parallels, BootCamp or other virtual software to run Windows only programs such as Microsoft Publisher. Because these Macs are now running a Windows operating system, they are now susceptible to Windows viruses. In addition, an Apple computer can become a "carrier" of a Windows-based virus. This virus would not infect the Apple machine, but could infect other Windows machines on your network if it were to send that virus via email or across the office computer network.

And Even More Threats...

Any software, plug-in or other 3rd party add-on that is installed onto any computer that connects to the internet can introduce its own security risks. One of the most common ways that the "bad guys" are able to attack a Mac is through browser applications and browser plug-ins such as Adobe Flash, Adobe Reader, Java and others. Just about every Mac user has all three of these plug-ins installed on their computers (and many more). These are a necessary part of business, but do introduce additional security risks for all computers.

The Human Factor

Although Apple Macs are less vulnerable to viruses, they are operated by flawed humans who can still be the victim of Trojan Horses, phishing and other online fraud. Your best bet is to keep everyone informed about online security risks in your business, no matter the computer they're using.

The Lighter Side:

PHILOSOPHY OF SPRING CLEANING



I don't do windows because...

I love birds and don't want one to run into a clean window and get hurt.

I don't wax floors because...

I am terrified a guest will slip and get hurt then I'll feel terrible (plus they may sue me.)

I don't mind the dust bunnies because...

They are very good company, I have named most of them, and they agree with everything I say.

I don't disturb cobwebs because ...

I want every creature to have a home of their own.

I don't Spring Clean because...

I love all the seasons and don't want the others to get jealous

I don't pull weeds in the garden because...

I don't want to get in God's way, HE is an excellent designer!

I don't put things away because...

My husband will never be able to find them again.

I don't iron because...

I choose to believe them when they say "Permanent Press."

DropBox – Is It Secure For Your Business?

A question that we often get around here is whether or not file-sharing services such as DropBox and Google Docs are secure enough for business. If you use any of these services for your business, here's the scoop...

Treat DropBox As A Public, Shared Environment.

DropBox type services are designed to easily share very large files – ones that are not optimal for e-mail because they're so huge. Examples include videos, audio files, large PDFs and graphics files. These services are typically free (or very cheap), and you shouldn't have the expectation of great security for this price.

But an increasing use of these tools, even for legitimate reasons such as collaboration, is putting a lot of private information at risk. According to a recent Ponemon study, 60% of organizations have employees that frequently put confidential files on services like DropBox without permission. In fact, companies such as IBM have banned the use of these services completely.

When Does Or Doesn't It Make Sense?

When you have a file that doesn't need to be secure and simply needs to easily and quickly get from point A to point B, then DropBox can be a viable solution. On the other hand, you should not send or store any sensitive files, such as contracts or financial statements, on DropBox. These services are also not safe for any files subject to government compliance regulations such as PCI, HIPAA, SOX, Sarbanes-Oxley or HITECH. These file-sharing solutions are NOT compliant.

What To Use Instead

If you need a secure way to store files for your company's use but still need the flexibility to email them to people outside your company, you'll want to take a look at the Frogworks Cloud9 Storage Solution. This solution will allow:

- Safe and secure collaboration
- Ability to work across platforms (Android/iOS) Mac/PC
- Continuous real-time back ups
- Comprehensive usage reports

Call Frogworks today at 240-880-1944 to get more information.

Shiny New Gadget Of The Month:

Intel Ultrabook Convertible

The Intel-based Ultrabook Convertible is one of the most cutting-edge on-the-go laptops to date. Quite simply, it's a laptop when you need it and a tablet when you want it.

Ultrabook with touch display, using Windows 8, delivers stunning graphics and the ultimate in precision and control. And unlike an iPad or Android tablet, this convertible turns into a powerful laptop in an instant.



Additionally, models with Intel Smart Connect Technology continually update your email and social networks even when your Ultrabook is shut down. You'll wake from sleep mode in less than 7 seconds and already be completely updated so that you can resume what you were doing in the blink of an eye.

And with Intel's Anti-Theft Technology, if your Ultrabook is ever lost or stolen, you can instantly disable the machine from anywhere, ensuring that your data is safe and secure!

Learn more today—call us at 240-880-1944.