



TECHNOLOGY TODAY



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

March 2016

Inside This Issue...

Spoofting emailPage 1

Bits and PiecesPage 2

Business EmailPage 3

Backup Questions.....Page 4

QuotesPage 4

Forget the wingtips.

Men are wearing sneakers, even to upscale meetings.

At the famed Barneys of New York, men's fashion experts say men can pair anything with the new lines of leather sneakers from sweatpants to a suit and they'll "look like a million bucks."

In fact, luxury sneakers now dominate men's footwear sales at e-commerce sites.

{Nothing about cowboy boots}

Spoofting and "free" email

As frequently happens when I start to write articles on topics I know about I realize I don't know what I thought I knew. And I'll admit that I'm a little weak in the world of email. Turns out for good reason. About an hour into my research I've figured out that it is way too complex for anyone but the most dedicated of techs. I marginally fit that definition but I'm too old to absorb the whole discussion.

That is fortunate for you. I can translate the deep geek to English. Here's what you need to know.

EMAIL SPOOFING: "Email spoofing is the creation of email messages with a forged sender address." *Wikipedia.com* [There's a very long complex discussion in Wikipedia with links to about five hours of research. Feel free.]

How it happens. Here's the bad news. You clicked on something in an email. Maybe it was a "Verify your PayPal account" or "UPS has a package for you, click here for tracking". Or any of a hundred other ways to get people to click on things. You've seen them, you've clicked on them. No one is perfect and it only takes once to get in trouble.

What happens next. Your email address is compromised usually by a Trojan virus and enough information is sent to the crooks they can use it to solicit money from your friends (the list of which they also acquire from your email address book). You may have heard of the scams: "I'm stuck in [insert foreign country here] and have lost my wallet, passport and money. Please send a money order so that I can get home" or something similar.

We see this several times a year and there's not much we can do for our customers after it has happened.

The fix? {Continued PG 4}

Bits and pieces

Companies try to create level playing field for hiring

Are you a smarter potential-employee if you studied at Harvard than if you studied online?

Or maybe you are a better pick for the job if you made the hiring manager laugh.

Then there are people who might be good if their names were not so hard to pronounce.

All these, considerations play into hiring in the real world, even with companies and people who want to be open-minded.

Some CEOs have realized these biases are not only unfair, but they don't result in the best employees.

Enter blind hiring or blind auditions.

Here employers try to eliminate every single consideration except quality of work. They don't want to know your name, see your resume or even meet you.

According to NPR, one blind audition site, GapJumpers.com, hosts blind auditions for software engineering, design, marketing, and communication. The site creator Petar Vujosevic says when a company posts a job anyone at all that wants to apply simply takes on a proposed project, probably not a simple one.

Instead of companies eliminating those who went to the wrong college, for example, it is performance that wins.

Employers say blind hiring reveals true talents and results in diverse hires.

The rising interest in anonymous hiring reflects growing awareness of unconscious bias, attitudes or stereotypes that could affect decisions. Even a person's name can affect how they're viewed and subtly prompt managers to make unfair decisions, says The Wall Street Journal.

Tech-industry recruiter Aline Lerner saw firms ignore talented technologists if they

lacked degrees from elite schools or experience with tech giants.

Lerner quit recruiting to build Interviewing Inc., a website that pairs interviewers with interviewees in chat rooms where they were encouraged to talk but not share their names.

Great \$10 bottles of wine

Howard W. Hewitt of Grape Sense says his column educates consumers on wine quality. He reports that people who want a great wine for \$10 have several good choices. His favorites in this category are Robert Mondavi Central Coast and Menage a Trois.

He cautions you not to pick a wine by its cute label or interesting name.

Menage a Trois is a mass produced wine that will surprise you with its balance, flavor, good finish, and ability to pair with food, he says. The label covers some 15 different wines and is one of the fastest-growing brands in the value category. It's all about red blends like Midnight and Silk at \$8.99 or less.

Mondavi's Central Coast scores big with its line varietals at \$9.99. The Cab tastes like Pinot Noir.

Other good \$10 wines include Bogle, Blackstone, Mark West, Mirrasou and Clos de Bois.



Spoofting and Spam in your business

I'm adamantly apposed to businesses using free email such as Yahoo or AOL. Even using Gmail, for your business, could be a problem. Also using Verizon.com or Suddenlink.com as your email address is problematic. Two reasons for this:

1—Control. We have a business partner who has [*business_name*]*@Verizon.net* as their email address. It is on all their marketing and has been in use for years. Now Verizon is dumping Verizon.net and shifting to AOL.com. So this business has a problem. If you don't own your own domain name and your own business email then it is just a matter time before there is a problem and it will be an expensive one to solve.

2—Appearance. I see [*business_name*]*@yahoo.com* and it is very hard for me to take them seriously. The appearance is unprofessional. It is not expensive to have your own domain name and, using Office 365, your own email address. It is also MUCH more secure.

Office 365 has become an extremely secure email system and in my opinion is where all businesses should be if they are not big enough to have their own mail systems.

This is not a very difficult thing for us to do. We have a lot of Office 365 clients so give us a call and we'll help you set it up.

Essential steps to protect your data

There are various ways to calculate the cost of losing work stored on computers. Perhaps the easiest way to get a gut feel for the cost is to think for a moment about how long it would take to replace lost work. How many people would have to spend how many days to create everything from scratch?

What would tomorrow look like if all your computers died tonight?

You will not know what approach is right for you until you have answered these questions:

How long can you go without the data that you lost?

How much data do you have and how often does it change?

How quickly will you need data restored?

What devices will you use?

How secure do your backups need to be?

How long do you need to keep the data?

One of the things we do well is assess backup needs and strategies. There are bulletproof backup processes that we can put together for you. It does not take long to work out the best system. **Friendly Backups** can save the day!!

Quotes

In one of English writer James Allen's books, he devotes the entire first chapter to beginnings, saying, in part:

Most beginnings are small, and appear trivial and insignificant, but in reality they are the most important things in life.

Without a beginning you could have the greatest idea in the world and you would still fail. A modest idea and an incomplete plan often produces success when accompanied by even an "insignificant" beginning.

It's not your job to like me, it's mine.
Byron Katie, co-author of *Loving What Is: Four Questions That Can Change Your Life*

An entire sea of water can't sink a ship unless it gets inside the ship. Similarly, the negativity of the world can't put you down unless you allow it to get inside you.
Goi Nasu, author of inspirational quotes



"My name is Debra and it's been 3 hours since I posted pictures of my cat, my grandchildren, my dinner, my..."

Spoofing and "free" email

{continued from Page 1}

How can I avoid my email being spoofed, you say?

Well my first answer is a quote from a Lifehacker.com article on email spoofing. You already know this answer:

As always, the weakest link in security is the end-user. That means that you'll need to keep your BS sensors turned all the way up every time you get an email you weren't expecting. Educate yourself. Keep your anti-malware software up to date.

The people doing this are part of a huge organized crime and the majority are from eastern European countries. Many of the tools used in these ventures are available for sale on various markets accessible through back end web sites. There are even 'help' desks for criminals who are not so technically capable. All of this is beyond the reach of U.S. law enforcement. There is a coalition of groups interested in stopping this sort of activity but on an international scale email spamming and spoofing is not today's top priority.

My recommendation for personal email is to use Gmail. (I'm talking about personal email, not business here.) It has the best security track record year over year. I've been using it for my personal email since it was in Beta mode and I've only seen the security get better. I very occasionally get what I would consider spam, a message I did not request or want. There's a button at the top of the Gmail screen that lets me report the message (and the sender) while it removes it to the spam folder. This happens maybe once a month and I get hundreds of emails into that box from technology lists I'm on.

Summary:

- 1 – Make sure your antivirus is working. (By the way we use, sell and recommend AVG CloudCare, the business version of AVG, for businesses and residential use)
- 2 – Pay attention to links all of the time but especially in emails from people you do not know.
- 3 – Consider using Gmail as the most secure service.

NOTE: If you have a business, take a look at my very different recommendation on Page 3.

Tom Schubert