

Healthy Living...

IT Wellness — Prevent the Spread of Viruses

We all know enough to follow good hygiene and general wellness practices to avoid spreading germs... washing our hands, coughing into our elbow, and keeping our hands away from our eyes and mouth. Most of us working parents remember the first time dropping off our child at day care and cringing when the first thing our child did was put a toy in their mouth. For this reason, many of us encouraged our children to use their pacifiers a little while longer to avoid germ objects making their way into their mouths. Of course, there's always the risk of the pacifier falling on the floor. Does the 3-second rule apply here?

Precautionary measures when it comes to personal health are second nature. We know how people spread viruses and we take measures to prevent them. Unfortunately, the same is not true when it comes to computer viruses. We know they exist and that they are harmful, but do we really know how they spread? Some ways may surprise you...

Email Attachments – Unfortunately, sometimes we receive viruses via email seemingly from people that we know and trust. Even when emails are extremely generic sounding and come with suspicious attachments, people often open them anyway since they came from a friend or from a trusted site. The golden rule is that if you don't know what an attachment is, don't open it (especially attachments with an .exe or .dll extension)! It's easy for a hacker to pretend to be someone you know.

Malicious Websites – Like it or not, you may become infected with viruses by doing nothing more than simply visiting a website. To stop these malicious websites, adjust the settings on your antivirus software and firewall so that no outside connections can be made and no programs can be installed without your permission.

Networks – Through no fault of your own, you may find yourself with a virus just by being connected to a larger network where someone else on this network downloaded a virus by accident. There isn't much you can do to safeguard yourself from these kinds of viruses; however, have your network administrator ensure that everyone's antivirus software is up to date so that the virus can be removed as quickly as possible.

Phishing Schemes – Identity theft is on the rise, and phishing schemes are the number one reason. A phishing scheme is when you receive an email from a legitimate looking website claiming to be your bank or credit card company. You freely provide your personal information without batting an eye. Often times, when you visit these sites, viruses are automatically installed on your computer. The smartest thing you can do is to simply call your bank or credit card company directly if you receive an email to confirm it's legit!

Infected Software – There are a plethora of free games and programs on the Internet, but they sometimes come with a price! If you happen to stumble upon a malicious website, you will unknowingly infect your computer if you download a free game or piece of software. Buyer beware...only download freeware or shareware from a trusted source.

(Continued on page 3)



What's New

February 1

Change Your Password Day

Join us as we make the commitment to stay safe online and change our passwords!

February 9

Webinar:

10-Minute Tech Tips: Phishing Lures

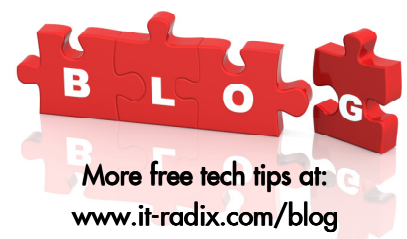
Register: www.it-radix.com/webinar
Starts @12:10 sharp

March 10

Client Appreciation Pancake Breakfast

Come enjoy an Office 365 presentation, visit with our IT Radix staff and build business relationships with other IT Radix clients.
www.it-radix.com/appreciation

If you would rather receive our newsletter via email, sign up on our website or send an email to resource@it-radix.com



Time for a Web Browser Wellness Checkup



For years almost all Windows users browsed the web using Internet Explorer—Windows' built-in web browser. Only hard-core computer "geeks" ever made use of third-party browsers. But times are changing. As a matter of fact, according to NetMarketShare's latest numbers, Internet Explorer is the second most popular browser with a 32% market share. A good margin behind Google Chrome, which grabs 47% of the desktop browser market.

But which browser is best for you? *Edge, Chrome, Firefox, Internet Explorer*

There is a common belief that Chrome is the most secure web browser. While it was indeed the first browser to take a hard line on security by outright blocking insecure content, it no longer stands alone in this arena. The top three browsers (Internet Explorer, Google Chrome and Firefox) all turn in very good scores when it comes to security. They also offer "privacy" modes to prevent tracking of your movement around the internet. One does, however, need to question the privacy provided by Chrome. It is, after all, written by a company that makes money on gathering user information.

Chrome gets high marks for its unified browsing experience. It is supported on just about every device out there—iOS, Android, Windows and Mac. And, when coupled with an online Google account, allows you to share many of your settings and favorites across all these devices.

All three of the browsers also have plugin capability, but Firefox does seem to win out in this area as there seems to be a far greater number of plugins for Firefox. Google is no slouch here as there are quite a few plugins for Chrome as well. Microsoft brings up the rear here as people are a bit slow to adopt Edge compatible plugins.

Speed is another measurement of a good browser and here is where the newest browser from Microsoft, Edge, seems to shine the brightest. While the other browsers are not necessarily "slow", Edge does seem to "edge" out the competition.

So, which is best? It really does depend. For the ultimate in security and a unified browsing experience, Google **Chrome** is the top choice. For speed and a wide array of plugins, **Firefox** would likely be your "go to." For the tightest integration into Windows as well as speed, **Edge** would be the winner.

The absolute most important thing you can do, no matter what browser you decide on, is to keep it up to date. The hackers are hard at work trying to exploit any flaw in these browsers, and the only way to stay ahead of the bad guys is to keep your browser, and all your software, up to date.

Do You Think IM Safe? Think Again!

Did you know that billions of instant messages (IMs) are sent each day in the United States alone? That means information of all kinds is being sent and received by your devices on a near constant basis. Some of that information is simple enough, a quick "Hey!" or "Did you see that email?", but some of that information is more detailed... "Hey real quick, I've got to access this report, what's your password?" or maybe, "Hey I've forgotten my password, I thought it was S3curityR!\$k, am I spelling that right?"



Messages like these are being sent back and forth every day so it's important to understand the risks of having instant communication at our fingertips. Just like a conversation, once your messages are sent, that information is out of your hands; and just like a conversation, your instant messages can be overheard too.

Whether a co-worker you didn't hear behind you just saw a message meant for a specific colleague or you've just received sensitive information (it could be something as simple as a name and a birthday), all of this data has to be transported throughout the world wide web to arrive in your IM client. And just like a verbal conversation, the Internet is full of listening ears, waiting to hear what you have to say.

Don't get us wrong... we're a part of those multi-billion IMs each day too, and we think it's a great technology. But, it's important to be mindful of what you're sending. Keep your IMs short, sweet, and to the point, and you're already putting your best foot forward when it comes to your cybersecurity wellness.

**OUR CLIENTS
SPEAK OUT:**

THE BUZZ

"As a care management practice serving the elderly population, it is paramount that our care managers have access to our clients' medical records at all times. IT Radix is the gold standard when it comes to competence, professionalism and efficiency in IT support. I wouldn't want to run a business without them!"

Deborah Vogt – Peace Aging Care Experts, Inc.

IT Wellness — Prevent the Spread of Viruses

(Continued from page 1)

Fake Antivirus Software – There are a number of free antivirus programs on the Internet, and a surprising number of them are fake. Only download antivirus programs from trusted sites or from websites that you know are completely legit. Unsure? Ask us!

Peripherals/Mobile Devices – When buying peripherals that connect with your computer, you may inadvertently infect your computer with a virus. There really is no way to stop such an infection from happening, but by keeping your antivirus software up to date you can ensure that you have the tools ready to go if you are infected.

When it comes to viruses, preventative care is critical! You are your No.1 defense when it comes to preventing the spread of computer viruses!



Proudly folded & stuffed by Park Lake School

SPECIAL OFFER

An Apple a Day Keeps the Doctor Away



Sign up for a year of IT Radix Management and Support during the months of **January, February and March**, and receive an Apple Store gift card.

Visit www.it-radix.com to learn more about what's included in each of these proactive maintenance plans. Offer for new managed service clients only. Some restrictions may apply. Call **IT Radix** today to learn more!

Protection from Insider Threats



The human body is amazing—all the various parts working together to live. White blood cells have the responsibility of recognizing and defending the body against foreign invaders. But what if the “invader” is something from within. A recent survey of organizations with 250 or fewer employees revealed that 38% of them had experienced an internal IT security incident in the past year.

Just like your body, you must protect your computer network from threats and the fact is that we are most vulnerable from threats from within. Why? It's simple, they already have access to your physical facilities and your computer systems. So, what do you do? The first step is match a person's access with their need to know. Many organizations have shared information storage areas. Access to the information should be segregated and set to match a particular person's need to do their job and nothing more. This access should be identified and documented in your organization's security policies. Many organizations simply ignore this step for convenience. The policy should clearly spell out who is authorized to have access to what information as well as the consequences of accessing information inappropriately. Remember that least privilege needs to be managed on an ongoing basis. Access and privileges should be updated whenever an employee gets promoted, transferred, or leaves the company altogether.

But the fact is that often people need access to information simply to perform their job. So, how do you prevent an employee who is authorized to access confidential information from maliciously abusing their authority? First, it helps to identify the typical motives which induce a person to abuse their access. These motives include fraud, theft of intellectual property or confidential information or intentional business disruption from a disgruntled employee. Quite often there are red flags that can help trigger the need for closer inspection or tighten security.

Your security program should look internally, in non-traditional ways, to help connect the dots. For example, HR data about sickness, vacation, benefit changes (e.g., divorce, child custody), or poor performance reviews could raise alerts when combined with external public data (e.g., bankruptcies, arrests, legal issues, or social media), that may increase a person's motivation to violate your security policies.

IT Radix recommends a strong backup of all critical data to help protect against intentional and unintentional acts that may result in business disruptions. A strong backup protects the data from deletion or corruption.

If you want to take matters a step further, technology exists to monitor and alert when internal suspicious activity occurs. We always encourage clients to ensure that employees are aware that such technology is in place and quite often, that knowledge is sufficient to stop most individuals. However, in the event it's not, the data loss prevention software can alert you if someone is accessing information in a suspicious way (e.g., downloading data to a USB key.) It can also record all or select actions performed on a computer.

Just like the human body adapts to change, organizations must adapt to ensure their information security program accounts for both insider and external threats. By analyzing all the information available, your organization will be able to identify network and behavioral anomalies and take action before any damage occurs.

"Wellness is the complete integration of body, mind and spirit—the realization that everything we do, think, feel and believe has an effect on our state of well-being." — Greg Anderson

“A good laugh and a long sleep are the best cures in the doctor’s book.”
— Irish Proverb

© Randy Glasbergen
www.glasbergen.com



“Doctor and physician are outdated terms. I’m your biological tech support specialist.”

From the desk of: Cathy Coloff
Subject: Be Well!

We’re into a relatively warm winter again and, unlike many, I’m wishing for snow. I enjoy cross country skiing and the warm winters have severely limited my cross country skiing opportunities. Of course, I could simply use my trusty old Nordic track to ensure my activity level stays up through the winter months but it doesn’t get me outside into the great outdoors. So, I’ve taken to just stepping outside for a minute every morning before I sit down to work in my home office. I usually wake between 4:30am and 5:30am, so some mornings, I can’t really see much when I’m out there until the motion sensor outdoor light gets triggered. I surprised a deer and myself once as it was meandering through our yard. The fresh air and the sometimes bracing cold jump-start my day and gives me a moment of peace before tackling the day ahead.

I always enjoy learning about people’s rituals that help them relax, stay focused, healthy, well and the like. Sometimes I give them a try—while some I enjoy, others don’t work for me. The same is true with technology. I’ve also discovered a number of cool apps that I enjoy and others that I don’t. These days, I’ve been enjoying a coloring app on my iPad or Surface with their Bluetooth pens. Sometimes I even go low tech and color one of the many beautiful adult coloring books on the market today. Relaxing and beautiful at the same time. How cool is that?



“Life is not merely being alive, but being well.”
— Marcus Valerius Martialis



Wacky Wellness Facts!

- Laughing lowers levels of stress hormones and strengthens the immune system.
- On average, women say 7,000 words per day and men speak just over 2,000.
- One in every 2,000 babies is born with a tooth already in place.
- Every square inch of human skin consists of 25 feet of blood vessels.
- A cough releases an explosive charge of air that moves at speeds up to 60mph. A sneeze can exceed speeds of 100mph.
- The eye of a human can distinguish between 500 shades of gray.
- In an average lifetime, a person has about 600 million breaths.



To Sit or Not to Sit

...That is the question! The average person spends at least 9 hours per day sitting. That’s more than half of your waking hours! Studies show that too much sitting is harmful...even if you exercise regularly. Being sedentary raises your risk of developing many serious health conditions and shortens your life expectancy.

But in today’s technology-centered workplace, where most office jobs require sitting in front of a screen all day, what’s a person to do? Well, the answer is...**STAND!** You actually burn 30% more calories standing than sitting, and moving throughout the day uses more energy than a continuous bout of physical exercise. So don’t be a sitting duck!

Today’s **Standing Desks** are an answer to this dilemma. They promote healthier behavior, better posture, increased circulation in your legs and help improve hip flexor mobility. Our team member, Amy, couldn’t agree more. She’s been using a standing desk ever since experiencing major back problems this past year. At the office, her standing desk accommodates dual monitors and easily pulls up and down depending on her preference. Amy feels more productive when standing...more awake and more energized. She feels when she’s multitasking and bouncing from task to task, that standing seems to improve her focus. She’s more in command of things with a better view of what’s happening in the office. The ability to switch back and forth between sitting and standing has made it much easier for her to alleviate and accommodate her back discomfort. When working from home, Amy uses a cardboard standing desk that is easy to set up and conveniently stores flat when not in use—a very cost-effective option for home use.

Need help planning your optimum workspace, whether you’re sitting or standing? Check out Ergotron’s workspace planner (www.ergotron.com/tools/workspace-planner). Enter your height and see optimum placement of your computer equipment.