

# Innovations

January—March 2010 Newsletter

## What's Inside....

The Internet can be a dangerous place!.....1  
Is your password keeping you safe?.....1  
Is the iPad just an oversized iPhone?.....2  
TrueCall Phone Screening.....4  
YoGen Hand Charger.....4  
FREE Network Assessment.....4

## St. Patrick's Day

### Common misconceptions

- ♣ **St. Patrick was Irish.**  
Believe it or not, St. Patrick wasn't Irish at all. He was born in Britain with the name Maewyn Succat.
- ♣ **St. Patrick was always a saint.** At a young age, Maewyn was enslaved and brought to Ireland where he stayed for over a decade. He became a priest when he escaped from Ireland. Later he changed his name to Patrick and returned to share his religion with the Irish. They later dubbed him a saint for his service.



www.history.com  
/content/stpatricksday/

Happy St. Patrick's Day!

## The Internet can be a dangerous place!

*The recently released APWG Phishing Activity Trends Report, for the third quarter of 2009, provides surprising insight into the startling facts about Internet threats. Implement policies to protect your company's confidential information before it is too late.*

**Startling statistics surface...** 48% of 22 million users scanned, had malware and the financial industry seemed to be the most targeted sector. 48% works when you are splitting a burrito with a co-worker, but these odds are not favorable for business decisions. Sneaky criminals can easily hide Trojans, malware and viruses in your computer if you visit websites online or if you click on links in e-mails.

Prepare yourself and your business against the very real dangers of the Internet. Know what to look for and implement safe surfing practices to promote your network security and the overall health of your organization.

### You wouldn't fish with a spoon, right?

No. So, don't expect everyone in your company to know how to safely use the Internet. Give them the facts and tools they need to succeed and keep your business safe.

## If 308 million password possibilities can be attempted in under 3 minutes, is your password keeping you safe?

*December 2009 a popular website named RockYou.com experienced a horrifying breach. A clever hacker managed to penetrate their systems and stole account information for 32 million users.*

### Social websites. A weakness for users?

RockYou and other social sites like FaceBook, MySpace, and LinkedIn, require personal information like your e-mail address, your full name, and sometimes even your birthday or address to verify you are

### Fight Internet scams with brain power.

Half of the battle is identifying scams and knowing what to do if your workstation is compromised. Take a moment to review these five steps to avoid online scams and infections.

- 1. Awareness is key.** It is important to understand that the Internet is not a theme park that is open for the public to explore. There are quite literally millions of ways you can fall into a trap online. For example, eBay scams or Phishing sites. Always research websites you want to visit.
- 2. Look for a working phone number.** If you need to make a purchase online, call the company first to ensure there are live humans on the other end of the line. Do not accept just leaving a message. Wait to hear back from a representative and ask questions regarding the company history or the product you need.
- 3. Check out the company name or site online.** Enter "[company name] scam" into Google, use Scam.com or Snopes.com to see if the company has been sited for scams in the past. If you get a slew of

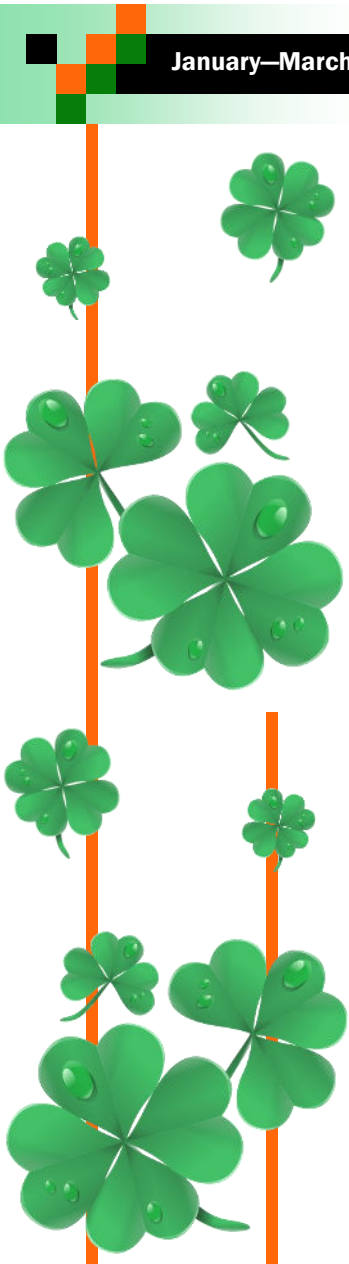
(Continued on page 2)

a real human. While this information seems pretty generic to users, thieves gather this data to build profiles on unsuspecting users. These profiles are ultimately used for identity theft or hacking personal accounts, such as your bank.

### Many people use weak passwords or the same passwords for multiple websites.

This is like leaving your car door open when you go to a baseball game. While there are many cars in the

(Continued on page 3)



## The Internet can be a dangerous place...

(Continued from page 1)

complaints and information back, this is a big red flag. Of course, some of the complaints and postings will be bogus so use your best judgment.

- 4. Trust your instincts.** If it doesn't feel right, don't do it! At the end of the day you want to keep your company information safe and to ultimately build a new vendor relationship, not create a massive problem for you to clean up. If it sounds too good to be true, it probably is.
- 5. If you think you have a virus or other infection, have it checked.** The first thing to do is unplug your computer from the network. If you have an infection, it may spread just like the common cold, to other workstations. Unplugging the network cable stops the hacker and isolate the issue to just your machine.

Now that you can identify, research, and stop scams, let's take a look at the most frightening trend.

**Do you use online banking?** If you have come to rely on financial services online, you may want to change your habits. Even if you dedicate

one computer in your office for financial transactions only, the risks are still high. Of the 22 million scanned computers in the APWG report, 1.7 million had banking Trojans or password stealers on their computers.

**Could your business survive if the bank account was cleaned out?** Truthfully, it doesn't matter how sophisticated banking security measures become, cyber criminals will always have a fighting chance due to the volume of computers in which they have already infected or embedded programs. These days, thieves are not easily identified with obnoxious pop-ups. They often infect a computer and sit quietly in the background collecting information without tipping off the user until they are ready to strike. This is why it is so important to stay educated, enforce Internet use policies, and scan your computers regularly to prevent downtime or costly data loss.

**Skeptical about the condition of your computers?** Take a look at our FREE Network Security Audit highlighted on the back page or give us a call now to schedule an appointment.

([www.antiphishing.org/reports/apwg\\_report\\_Q3\\_2009.pdf](http://www.antiphishing.org/reports/apwg_report_Q3_2009.pdf))

## Is the iPad just an oversized iPhone?

*The Apple iPad, released this quarter, is a fantastic innovation in computing, not just an enlarged iPhone.*

This new device is paving the way for future multi-touch computing products. The iPad offers a handful of embedded applications for users to navigate e-mail, contacts, calendars, photos, videos, books, music, and more.

**Physical features:** The iPad comes equipped with a 9.56 x 7.47 inch LED-black lit IPS display. This screen offers remarkably crisp graphics for users to enjoy photos and videos. The iPad has a 1/2 inch depth and 1.5 to 1.6 pound weight, giving users the versatility they crave.

**What's inside:** The iPad comes with a 16GB to 64GB flash drive and a built-in rechargeable lithium-polymer bat-

tery that lasts up to 10 hours of surfing the web on Wi-Fi, watching videos, or listening to music.

**Accessories:** The iPad keyboard dock charges the iPad and offers a full-size keyboard just like a laptop. This slick docking station uses a USB power adapter and can sync to your computer or other accessories like a camera or stereo.

The iPad case, not only protects the iPad, but can be used in various positions to view photos with friends, run a slideshow for meetings or even watch videos anytime, anywhere.

**Faults:** The chief complaint about this new product is, the Internet browser doesn't support Flash. OUCH! In addition, there is no camera, USB, or phone features so users will still be managing their laptop and cellular devices too.

**Price tag:** This new device comes in at a stunning \$499 to \$829 depending on the flash drive and data plan, if applicable. This is quite an affordable price for such a niche market product.



## Is your password keeping you safe?...

(Continued from page 1)

lot, a thief will steal the one that is easiest to access. If your password is easy to guess or is the same on your social sites and your e-mail or even your banking website, hackers will simply plug in the password over and over to see what they can compromise. In this digital age of instant gratification, even hackers are automating their processes to increase efficiency.



word and the special characters in the sentence to create an impenetrable password you can chuckle about each time you use it, “Md,J,h500B!” Now that is a password hackers won’t find in the dictionary. Keep in mind, the more bizarre your sentence is, the more likely you are to remember it.

### Let’s take a look at password trends.

Just reviewing statistics pulled from the 32 million folks unfortunately entangled in the RockYou hack, we can clearly see a poor password trend on this social site.

- ♣ Roughly 30% of users chose passwords whose length is equal or less than six characters.
- ♣ Almost 60% of users chose their passwords from a limited set of alpha-numeric characters, meaning letters or numbers next to each other on a standard keyboard.
- ♣ Nearly 50% of users used names, slang words, dictionary words or trivial passwords they could easily remember.
- ♣ The most common password among the 32 million RockYou users compromised was “123456”.

(Impervia.com white paper titled Consumer Password Worst Practices)

**Hackers love password checkers.** Did you know that password checking software programs can run all 308 million possible letter combinations for a six letter password (using all upper or all lower case letters) in under 3 minutes (www.hq.nasa.gov)? Quite impressive, but also startling.

You can protect yourself with these three golden rules of creating strong passwords:

1. Make sure your password is 8 or more characters in length.
2. Use a mix of the three basic mediums available: letters (both upper and lower), numbers, and special characters like !@#%&^?\* or &.
3. Don’t use only names or words from the dictionary, they are easily identified by hackers.

Following these three simple criteria is easy, but sometimes the password you come up with is difficult to remember, right?

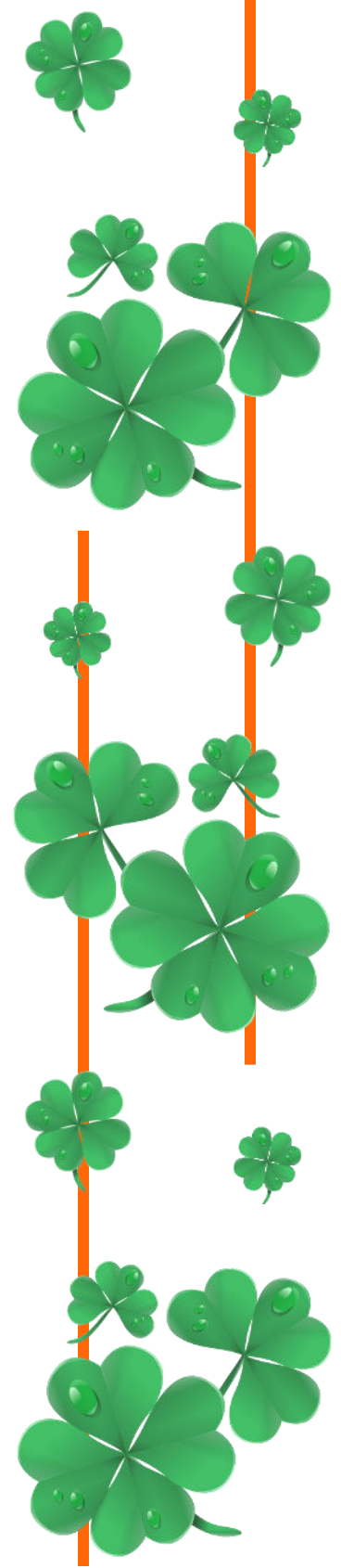
**Try using first letter mnemonics to fool those evil hackers.** Think up a short sentence you can easily remember like, “My daughter, Joy, has 500 Barbies!” Then take the first letter of each

**What does this mean for users?** Wimpy, simple, weak passwords won’t keep your private information safe. If you have to, write more complex passwords and keep them in your wallet or purse. Better yet, jot down reminders of what your passwords are just in case someone gets hold of your cheat sheet.

## Top 20 passwords found among 32 million users

If your password is on this list, you may as well post it on your Blog.

- |              |              |             |
|--------------|--------------|-------------|
| 1. 123456    | 8. 1234567   | 15. Jessica |
| 2. 12345     | 9. 12345678  | 16. Lovely  |
| 3. 123456789 | 10. abc123   | 17. michael |
| 4. Password  | 11. Nicole   | 18. Ashley  |
| 5. iloveyou  | 12. Daniel   | 19. 654321  |
| 6. princess  | 13. Babygirl | 20. Qwerty  |
| 7. rockyou   | 14. monkey   |             |



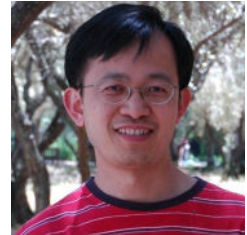


**eSudo Technology Solutions, Inc**  
**1440 Koll Circle, Suite 102**  
**San Jose, CA 95112**  
**Phone/Fax: (408) 404-6960**

**www.eSudo.com**  
**email@eSudo.com**

*“We make all of your  
computer problems go  
away without the cost of  
a full-time I.T. staff”*

*Ask us about our fixed price service  
agreements — Computer support at a  
flat monthly fee you can budget for!*



## Inquiring Minds...

**No telemarketing calls will interrupt your corned beef and cabbage this St. Patrick's Day.** Where caller ID fails, this new gadget picks up the slack. Now, you don't have to wait for unknown callers to leave a message just to find out who they are. You can have an automated system request that unrecognized callers identify themselves without even picking up the phone. A U.K. based firm trueCall Ltd. displayed their TrueCall product at the 2010 Consumer Electronics Show.

**Features...** This fancy tool is easy to setup, is packed full of features, and is compatible with a variety of phone systems and providers. The Shield function asks unidentified callers to press a number to continue before even ringing your phone. This eliminates those annoying automated call programs that give you a recorded message and then ask you to press a number to speak to a live operator. The Star and Zap feature holds your list of welcome or unwelcome callers' phone numbers so you don't have to answer the phone for your obnoxious uncle Herbert. The Call Screening feature sends all unrecognized numbers to the built in answering machine and the Anonymous Caller Reject will simply turn away callers who withhold their numbers from the system.

**TrueCall also has an Internet Control Panel** that is included free of charge the first year of service. You can view your call log and edit settings from any computer online. If that is not enough, there are a ton of other features to explore and even a few optional extras to fit your needs. Visit [www.truecall.co.uk](http://www.truecall.co.uk) online today to take a peek and rid yourself of telemarketers once and for all.

**100% green energy device charger!** Last year we saw countless advertisements and articles about how some company was “going green”! Keep your eyes peeled because 2010 will be chocked-full of manufacturer releases boasting their latest efforts for green products. The YoGen hand charger caught our eye. Basically, you use your hands to charge small portable devices. This small tool provides users with a remarkable way to charge their iPod, iPhone, cell phone, navigation unit, PDA, MP3, Bluetooth headset or even digital camera with an uninterrupted connection and no down time.

**How does it work?** Simply plug the YoGen hand charger into your device and tug on the cord for a few minutes. Pulling the handle creates energy for a charge even on the first pull and the device will be charged faster than using a standard AC wall charger. This type of product is fantastic for traveling, long events, and emergency situations. The YoGen is easy to use, it is human powered, 100% green, and gives you outlet-free mobility for roughly \$40.00. Wow! What a find!

## Rely On eSudo!

Imagine a hacker obtained access to your company information, client data, or private financial documents. An invasive attack could bring down your network and no one would be able to access e-mail or files until the breach was resolved. Could your company survive? Don't wait to find out. Enforce a strong password policy that triggers users to change their passwords each quarter or when suspicion rises.

Give us a call today to set up your **FREE Network Assessment**. We will identify potential threats to your network, suggest changes to help you safeguard your network and prevent downtime, as well as employ a password change policy.

**Focus On running your Business... Not your Network**

**(408) 404-6960 ♣ Email@eSudo.com**