MARCH 2015

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

SmartPath TECHNOLOGIES
Business Computer and Network Specialists

The Smarter Path

"As a business owner, I know 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!"

- Willie Kerns, SmartPath Technologies

What's Inside:

(270)238-8997

Thank You for the Referrals

In the last month we have given hundreds of dollars to our clients for referrals. Would you like some FREE money. All you have to do is refer a new client to us. Once we have our first meeting with them, we will send you $25.00 gift card. If that customer becomes an ITWorks client, we will then send you another $50.00 gift card. Keep them coming!

Pop Quiz: You Just Discovered One Of Your Employees Had Their Laptop Stolen...

Quick, What Do You Do?

Over the last couple of months, I've come across some alarming statistics that you should know. There are 12,000 or so laptops found in US airports each week and 62,000 lost electronic devices recovered from New York's metropolitan buses, taxis, trains, and stations each year! The bottom line is no matter how careful you are with your laptop, mistakes occur and losing a laptop (or having one stolen) is likely to happen to you or your employees at some point tin time. In the hands of a relatively unsophisticated hacker, all of your laptop information can be siphoned off, allowing an open back door into your network. This is akin to giving a thief the key to your office and the code to deactivate the alarm, imagine the embarrassment of having to contact all of your customers to let them know THEIR confidential information may be compromise because one of YOUR unsecured laptops is in the hands of a criminal!

Asking employees to be more careful about where they keep their laptop IS a good step in the right direction, but accidents happen and thieves are always on the prowl. That's why it's so important to take measures to lock down and secure any mobile devices you and your staff use to access your company's network. Here are just a few things:

Encrypt All Information— Drive encryption software such as BitLocker can secure all the data on your hard drive. Also, check your computer to see if it has a Trusted Platform Module (TPM) chip ally more secure that those without TPM.

Multi-Level Access Security– Don't rely on passwords to keep your laptop safe. Hackers can usually break most passwords in a few hours. We recommend adding a second way for people to prove that they are who they say they are BEFORE they are able to log in. Some people use smart cards to do this, but fingerprint pads are gaining in popularity.

Log/Back-Up Information– It's critical to log and back-up all information on business laptops to ensure smooth operations in the event of loss or destruction. We can automate the backups so they are done ON SCHEDULE and in a way that won't interfere with the use of the laptop.

The Right Response—What happens when an employee loses a laptop? Do you have a next action plan in place? If not, we suggest calling us immediately to report the loss. The sooner we know, the sooner we can take preventative actions to lock that laptop out of the network. A blame culture where people are afraid to report losses is much worse for security.

Take time NOW to secure your laptop and limit the damage to your business if it happens . We specialize in securing business data like yours, and making sure it is available whenever you need it, so give us a call at (270)238-8997 to discuss encryption options and how to make your business network more secure.

The Lighter Side…

Endorse This Skill: Jihad

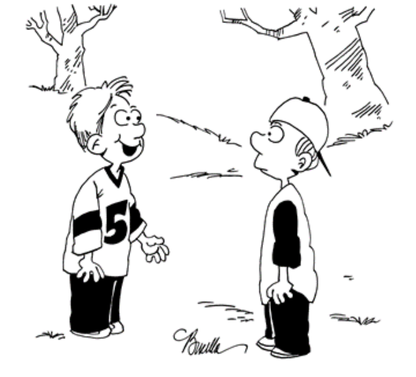
We endorse the skills of our coworkers, friends, acquaintances and other connections on LinkedIn all the time. But what would you do if one of your connections listed “jihad” as one of his skills? Unless you’re in the business of extremism (you’re probably not), you’re likely to slink away quietly and alert LinkedIn admins.

Well, one senior Taliban commander decided to update his LinkedIn profile with this very “skill.” Specifically, he listed “jihad and journalism.” This particular terrorist leader, Ehsanullah Ehsan, even lists himself as “self-employed.”

Unfortunately (or fortunately), when LinkedIn was contacted by the *Telegraph* for further information, the social media company decided it was best to take the account down.

There has been some chatter as to the legitimacy of the account. The profile’s distinct lack of Taliban propaganda and recruiting information suggested it wasn’t operated by the terrorist leader himself or anyone in a significant leadership position.

Of course, as a terrorist leader and all-around terrible human being, he has more pressing things to worry about other than a suspended LinkedIn account, such as a $1 million bounty placed on him by Pakistani officials.



“You know what I just noticed about playing outside? No pop-up windows.”

Overlooked, Low-Tech Tips Everyone Should Know To Keep Confidential Documents... Confidential!

As a smart business owner you have locks on all of the entryways into your office, you have surveillance cameras or security alarms in place, and your network security is bullet-proof (especially if you’re one of OUR ITWorks client). But another often overlooked security breach happens right on your own staff's desks. If you get a lot of in-office traffic, this could be on of the largest risks in your security plan. Here are four things you should avoid to keep you confidential information out of prying eyes.

1) Writing passwords on sticky notes—This is probably one of the biggest offenses—passwords and key system information written on notes and stuck on computer monitors. Anyone in the office after hours can access confidential files, steal information, and use it to compromise an account. But if you just hate remembering all those passwords, then install the password management tool from roboform.com
2) Storing credit card orders or contracts in paper folders—Not only does this expose you to having this information stolen, you could end up getting a lot of bad press if your customers credit cards get stolen thanks to a security breach in your office. The safest bet is to scan, encrypt and store such documents electronically, and then shred the originals. Companies like Iron Mountain will store them for you off-site, but scanning and storing them electronically is a much more cost-effective means for not only keeping them, but accessing them later on.
3) Leaving sensitive documents on the desk— Many times detailed client contracts with billing terms or other critical data are left out overnight. The information might be used for ill-gotten gains by cleaning staff or staff in the office. What an embarrassing situation this could cause! Make sure you lock your office at night or when you’re going to be away for any length of time.
4) Forgetting the printer— Most offices have printed documents sitting around all day and sometimes overnight before the owner picks them up. There are also sensitive documents that are forgotten and left to pile up. After your employees finish with the printing jobs, they need to be mindful of any documents that were printed, even the ones that aren’t needed , and dispose of them appropriately.

Whether formal of informal, training your staff to handle documents properly is important to avoiding a load of problems. If you’d like information or advise about virtual filing systems, password protection services, high-tech whiteboards, or using printers more effectively, contact us now at (270)238-8997. We can help you get started today.

Did You Know:

1. The national symbol of Ireland isn’t the shamrock. It’s the Celtic harp.
2. The “Guinness Book of World Records” was created by Guinness brewery employees.
3. The color that was originally associated with Saint Patrick wasn’t green, it was blue**.**
5. Only 9% of the Irish population are natural redheads
6. Cats now outnumber dogs by two to one as Ireland's most popular pet
7. Irishman James Hoban designed white house
8. The term ‘boycott’ comes from Irishman Captain James Boycott
9. Ireland’s oldest pub, Sean’s Bar, was founded some 900 years ago
10. The longest place name in Ireland is Muckanaghederdauhaulia

MIKE MICHALOWICZ (pronounced mi-KAL-o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford—a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group, a consulting firm that ignites explosive growth in companies that have plateaued; a former small-business columnist for *The Wall Street Journal*; MSNBC’s business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book *The Toilet Paper Entrepreneur*. His newest book, *The Pumpkin Plan*, has already been called “the next *E-Myth*!” For more information, visit http://www.mikemichalowicz.com/.

Shiny New Gadget of the Month

The Withings Activité Pop

Lately, it seems the tech world has been inundated with wearable devices, from fitness trackers to smartwatches. They offer a number of useful features, but they also lack in elegance. They are often bulky, ordinary, complicated and—in the case of smartwatches—have less than desirable battery life.

This is where the Withings Activité Pop comes in. It looks like a classy watch on the outside, but on the inside it's a very different story. It's an activity tracker, verging on expressing itself as a smartwatch.

From the smartphone app, you control everything, from the analog dials to your activity goals. The watch face features a secondary dial that tracks your activity—from 0% to 100%—for the day. It's simple and straightforward. It's water-resistant up to 30 meters and available in three colors: azure, sand and shark gray. It's currently available at Best Buy, in-store and online.

Top Mistakes That Make You A Prime Target For Identity Theft

The numbers are staggering: according to the 2014 Identity Fraud Report, identity theft affected a whopping 13.1 Million consumers and businesses. Identity theft occurs when someone steals your name, social security number (SSN), bank account number, or credit card to open accounts, make purchases, or commit other fraudulent crimes.

The methods identity thieves use include low tech strategies (like going through your trash can, also know as "dumpster diving") to highly sophisticated phishing scams that include cloned PayPal or bank websites that trick you into giving your username, password, or account number. Other ways included:

- Stealing records from an employer or bribing an employee who has access to the records.
- Hacking into the company's employee records.
- Stealing mail, such as bank account or credit card statements, tax documents, pre-approved credit cards, or new checks.
- Abusing their employer's authorized access to credit reports.

Once someone has stolen your identity, they can use your credit cards or bank account to purchase expensive consumer goods like computers and electronics that can easily be resold for cash. They can also open and charge up new credit cards, which can be a real mess to straighten out with vendors and credit reporting agencies. Other criminal activities include taking out auto loans in your name, opening a new phone or wireless service in your name, or writing counterfeit checks to drain your bank account. Some have even used it to file for bankruptcy to avoid paying debts they've incurred, or to avoid eviction.

Never give your personal information, Social Security number, credit card number, or bank account numbers over the phone or online unless you know for certain you are dealing with a legitimate company. Make sure your employees are given an AUP (acceptable use policy) that educates them on the dangers of phishing scams and spam e-mails designed to either trick you into giving your information or installing a virus that secretly steals the information stored on your PC without your knowledge. You can recognize a secure website, as it has an https:// at the beginning of the web address (regular web sites only have http:// and no "s") at the top of the page on which you are submitting your information. It also must have a picture of a lock in the bottom right corner of the page. If you don't see both of these measures in place, do not submit your information.

And even if you DO see this, use a credit card instead of a debit card or pay by check option because you'll get security protection from your card's issuer. Visa, MasterCard and American Express all have a zero liability policy. If you notify the bank of unauthorized transactions, you pay nothing. And some credit card companies offer one-time use numbers to prevent someone from stealing your account number and using it for unauthorized charges.

Shred all medical bills, financial statements, credit card applications, tax statements, or any other mail that contains confidential information about you before you throw them into the trash.

Never open e-mails or attachments from e-mail addresses you are unfamiliar with, and NEVER respond to e-mails that ask you to verify your account information because your account is being closed, suspended, or charged. If you want to verify this, call the bank or the company to see if it was a legitimate e-mail.

If you see any unexplained charges or withdrawals from your bank accounts, if you receive credit cards that you did not apply for, or if you start receiving bills or collection letters for items you have not purchased, someone may have stolen your identity. Always follow up with the business or institution to find out exactly what is causing the situation as quickly as possible. The faster you act on identity theft, the easier it will be for you to clear your name.

SmartPath TECHNOLOGIES
Business Computer and Network Specialists

78 Ash St
Calvert City, KY 42029
(270) 238-8997

Innovative Criminals: Cyber Security for 2015

Data breaches, identity theft, credit card theft makes today's businesses be in a position that's very uncomfortable and unfamiliar to them.

Do you know what you would do if your computer network was the target of an invasion similar to the incident Anthem Insurance recently faced?

We'll provide lunch for you, and guest speakers will show you what your biggest threats are and how to stop them BEFORE it happens.

Sponsored By:

WOW!
PADUCAH
BANK
MEMBER FDIC

<u>Join us on</u>

Date: March 26, 2015 f
Time:11:00 AM to 12:30 PM
Location: Paducah Area Chamber of Commerce
Register at: www.smartpathtech.com/seminar