SmartPath TECHNOLOGIES
Business Computer and Network Specialists

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

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!"

What's Inside:

270-238-8997

SmartPath Employee Spotlight

Ira Morris is originally from Rockford, Illinois, where he received his Associates Degree in IT Security and Data Assurance from Rock Valley College. He began in the IT industry over 15 years ago with data entry, working his way up to Incident Management, before moving to Kentucky to become part of the SmartPath Technologies team. His varied experience in all levels of IT, makes him a great fit for our customers. In his spare time, Ira loves to scuba dive and visit his family.

The 5 Most Dangerous Pieces Of Information To Give In An E-mail

In the book *Spam Nation,* investigative journalist and cybersecurity expert Brian Krebs revealed the single most effective (and relied upon) way cybercrime rings gain access to your bank account, credit cards and identity. Ready for it? E-mail.

Whether it's opening an attachment infected by a virus, or a phishing scam where you unknowingly give up your login to a critical web site, e-mail still remains the most popular and reliable way digital thieves can rob you blind, steal your identity and wreak havoc on your network. Worst of all? You're INVITING them in! While there are a number of things you need to do to protect yourself, here are five pieces of information you (and your team) should NEVER put in an e-mail.

1. **Your social security number.** Think of this as your "bank account" number with the government. You should never e-mail this to anyone because it can be used to open credit cards and steal your identity.

2. **Banking information.** Your bank account numbers, routing number and online banking login credentials should never be e-mailed. Further, avoid sending a voided, blank check as an attachment to an e-mail.

3. **Your credit and/or debit card information.** NEVER update a credit card via an e-mail! If you need to update a card with a vendor, there are two safe ways to do this. The first is to log in to your vendor's secured site by going to the URL and logging in. Do NOT click on a link in an e-mail to go to any web site to update your account password or credit card! Hackers are masters at creating VERY legit-looking e-mails designed to fool you into logging in to their spoof site, which LOOKS very similar to a trusted web site, to enter your username, password and other financial details, thereby gaining access. Another way to update your account is to simply CALL the vendor direct.

4. **Login credentials and passwords.** You should never share your passwords or answers to security questions with anyone for any site, period.

5. **Financial documents.** An ATTACHMENT that includes any of the above is just as dangerous to e-mail as typing it in. Never e-mail any type of financial documents (or scans of documents) to your CPA, financial advisor, bank, etc.

Remember: Banks, credit card companies and the government will never ask you to click a link to provide them with any of the five items above. If you get an e-mail requesting you to update any of the above information, there's a good chance it's a phishing e-mail from a hacker. Don't be fooled!

Fresh out of business school, the young man answered a want ad for an accountant. Now he was being interviewed by a highly agitated, arrogant little man who ran a small business that he had started from scratch.

"I need someone with an accounting degree," the man said. "But mainly, I'm looking for someone to do my worrying for me."

"How's that?" the would-be accountant asked.

"I worry about a lot of things," the man said. "But I don't want to have to worry about money. Your job will be to take all the money worries off my back."

"I see," the accountant said. "And how much will my position pay?"

"I'll start you at 85,000," responded the owner decisively.

"Eighty-five thousand dollars!" the accountant exclaimed. "How can such a small business afford a sum like that?"

"That," the owner said, "is your first worry. Now get to work."

Vacation Alert!
The ONE Thing You And Your Employees Should NEVER Do When On Vacation

'Tis the season when you and your team will be taking a little time off to head to the beach or your favorite vacation spot, and while we know we *should* completely disconnect from work, most of us will still check e-mail and do a little work while away — and that could end up causing some issues if you're not careful while working remote.

So before you head off to have a little fun with your laptop tucked under your arm, keep this in mind: never automatically connect to "any available network." Not all Internet connections are secure, so if you're going to log in to the company's network, e-mail or other critical cloud apps that are hosting sensitive information, ONLY do so on a trusted, secured Wi-Fi and NEVER a public one. We recommend investing in a personal MiFi device that acts as a mobile Wi-Fi hotspot IF you're going to be traveling a lot and accessing company info.

Second, turn off the ability to automatically connect for all of your mobile devices and laptops. You will still be able to connect manually, but it will prevent your laptop or device from connecting to a questionable network without your consent or knowledge.

Finally, disable all printer and file-sharing options on your mobile devices. This is another way hackers can gain access to your network. In an ideal world, you and your employees would take a true break from work, but if they aren't able to completely detach themselves, then at least require them to stay safe using the above tips.
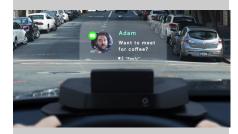
Shiny New Gadget of the Month

Navdy

Many of us realize how dangerous it is to check e-mail or text messages while we're driving, but we don't feel like we can afford to ignore our phone. Brand-new product Navdy to the rescue!

Navdy is a transparent Head-Up Display (HUD) that projects information as if it's floating six feet in front of you. It's very similar to what commercial airline pilots use. Navdy works with any car, and with all iPhones and Androids.

Using the apps you already have on your phone, and with no service plans required, Navdy allows you to focus on the road and not on your phone.

As a phone call comes in, Navdy's built-in camera allows you to simply swipe in midair to answer calls (or dismiss them), so you no longer have to fumble with buttons or touch screens. Plus, Navdy's voice recognition uses the voice commands you're already familiar with, whether you use Google Now or Siri.

Any notification on your phone (such as text messages or social media) can be played, read aloud or disabled, based on your preferences. Navdy even allows you to keep your teenagers safe by giving you parental controls.

The product is rumored to retail at $499, but is available now for pre-order for $299. Just visit their web site at: www.navdy.com

7 Secrets To Finding *Relevant* Information Online

Have you ever run into a virtual wall when searching for information on the Internet? With billions of websites online, finding good, relevant information online can sometimes be akin to finding a needle in a haystack. But take heart! Here are 7 little-known secrets that will help you find what you are looking for in no time at all.

1. Use the "Advanced Search" tool

Almost all search engines have an "advanced search" tool that will provide you with more options for filtering information and websites. This will help you narrow down your search and eliminate irrelevant, off-topic websites.

2. Search with a phrase in quotations

Putting quotations around a phrase will tell the search engine to look for that exact phrase or name instead of each individual word. For example, if you were looking for a chocolate cake recipe, type "chocolate cake recipe" in the search window with the quotes around it. If you left the quotations off, you might get recipes for other cakes or chocolate candy in general because the search engine will look up the words separately: chocolate cake recipe

3. Use synonyms

If your search does not produce the results you want, try synonyms. For example, a dog is also a pet, canine, mutt, pooch, and man's best friend. Use your Microsoft Word thesaurus tool or Merriam-Webster Online to find synonyms for your search term.

4. Use a plus or minus sign

This trick will allow you to narrow down a larger category. If you were looking for a roadside café in Atlanta, you would type in "roadside café + Atlanta". This will allow you to search on a specific set of keywords that might not be strung together in one phrase as mentioned in tip #2.

This also works in reverse with a minus sign (-). If you wanted to find all roadside cafes that were NOT in Atlanta, you would type in "roadside café - Atlanta".

5. Just search the domain name

If you know the website you want but can't seem to find the information you are looking for, you can tell the search engine to search for a specific keyword or phrase within that site. Simply enter the search term you are looking for followed by the word "site" and a colon, and then by the domain name.

For example, if you wanted to find information on spam filter updates for Microsoft Outlook, enter this: spam filter update site:www.microsoft.com

6. Eliminate inappropriate content

To eliminate adult sites clogging your search results, simply activate your favorite web browser's adult filter setting. MSN has a SafeSearch option on its settings page and Google's can be found in their advanced search option. It's not 100% accurate but it will eliminate the most obvious sexually explicit websites from your search.

7. Use your search engine's categories

Many search engines offer specialized areas such as news, video, audio, pictures, local, and shopping related categories. If you know you are looking for a picture, choose the appropriate category and your chances of finding what you want increase significantly.

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

SmartPath Technologies Will "Show You the Money!"

Our business is built off of referrals – it's the best "atta boy" we can get, and it lets us know our clients see enough value in what we do to recommend us to someone else who is suffering from IT and technology woes. The best part is – we'll pay for your referrals, no strings attached. Not only will we pay for them – we'll pay ANYONE in your office who refers us….it doesn't matter if it's an assistant, receptionist, or janitor. They can all get free money just from telling other businesses about SmartPath! Here's how…

Refer another business with at least five computers to us. We'll immediately send the referrer a $25 gift card AND we'll provide the business they refer to us with a free network audit and two hours of free service, a combined value of almost $500. We'll then analyze and review the audit with the business. It get's better…

If the business you refer ultimately decides to retain us and signs a service agreement, we'll pay $25 for each computer at the business. If they have 5 computers, you get $125. If they have 15 computers, you get $375, and if they have 20 computers you get $500 in CASH. There is no limit to the amount of money you can make from a single referral AND you can make as many referrals as possible every month.

Please make sure all members of your staff are aware of our referral program! It's been a great way to provide some much needed extra $$$ to staff members whom can really use it. Most office staff aren't aware they can have this opportunity, so please make sure they are informed.

Where Technology and Dependability come Together: www.smartpathtech.com