TECHNOLOGY UPDATE

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

Fake Apps Stealing Identity

WHAT'S NEW

B4 Networks welcomes Kwik Mix Materials LTD. as their new client.

Check out their profile on Page 4

FEBRUARY 2017

"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!"

Bryan Lachapelle, B4 Networks Inc.

B4 Networks Inc.
170 Hwy 20 W, Unit 3a, Box 249
Ontario, L0S 1E0
Tel: (905) 346-4966

Ryan loved tweaking photos on his Android phone.

He'd heard rave reviews from his friends with iPhones about Prisma, a new iOS app for image editing. So when he heard Prisma would soon be released for Android, he logged in to the Google Play Store to see if it was there yet.

To his surprise, he found one that looked just like what his friends were describing. Delighted, he downloaded and started using it. Meanwhile, the app—a fake—was busy installing a Trojan horse on his phone.

When he got to work the next day, he logged his phone into the company network as usual. The malware jumped from his phone to the network. Yet no one knew. Not yet, but that was about to change...

Fake apps exploded onto iTunes and Google Play last November.

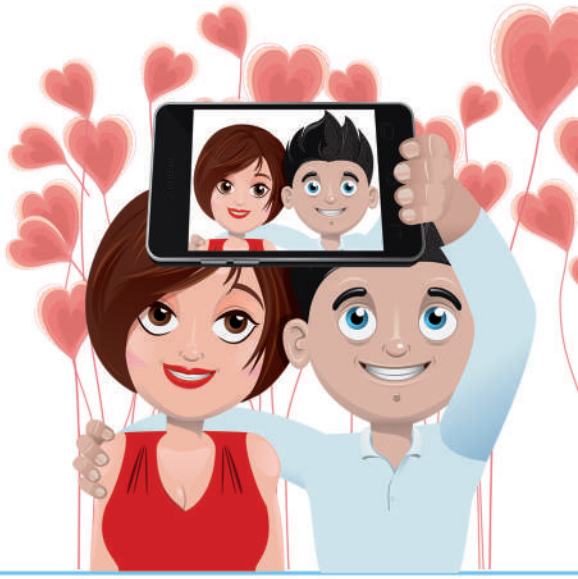
Now, this isn't necessarily a true story (at least, not one we've heard of—yet...), but it absolutely could have been. And similar situations are unfolding as you read this. Yes, possibly even at your company...

Fake apps exploded onto iTunes and Google Play last November, just in time for holiday shopping. Apple "cleaned up" iTunes in an effort to quell users' concerns, but hackers still find workarounds.

Unfortunately, these fake apps pose a real threat to the security of your network. Especially if your company has anything but the strictest BYOD (bring your own device) policies in place. And the more your network's users socialize and shop on their smartphones, the greater the risk of a damaging breach on your network.

Fake apps pose a real threat to the security of your network.

Fake apps look just like real apps. They masquerade as apps from legitimate merchants of all stripes, from retail chains like Dollar Tree and Footlocker, to luxury purveyors such as Jimmy Choo and Christian Dior. Some of the more malicious apps give criminals access to confidential information on the victim's device. Worse yet, they may install a Trojan horse on that device that can infect your company's network next time the user logs in.



Fake Apps Stealing Identity (continued from page1)

So what can you do?

First, keep yourself from being fooled. Anyone can easily be tricked unless you know what to look for. Take the following advice to heart and share it with your team:

Beware of Fake Apps!

In case you weren't aware, one of the latest and most dangerous Internet scams is fake apps. Scammers create apps that look and behave like a real app from a legitimate store. These fake apps can infect your phone or tablet and steal confidential information, including bank account and credit card details. They may also secretly install on your device malicious code that can spread, including to your company network.

Take a moment and reflect on these five tips before downloading any app:

1. **When in doubt, check it out.** Ask other users before downloading it. Visit the store's main website to see if it's mentioned there. Find out from customer support if it's the real McCoy.
2. **If you do decide to download an app,** first check reviews. Apps with few reviews or bad reviews are throwing down a red flag.
3. **Never, EVER click a link in an e-mail to download an app.** Get it from the retailer's website, or from iTunes or Google Play.
4. **Offer as little of your information as possible** if you decide to use an app.
5. **Think twice** before linking your credit card to any app.

Get professional help to keep your network safe.

Most importantly, get professional help to keep your network safe. It really is a jungle out there. New cyberscams, malware and other types of network security threats are cropping up every day. You have more important things to do than to try and keep up with them all.

Here is what a client is saying about us:

On a daily basis, B4 Networks does a lot for them, including:

- **Monitoring backups and systems** to ensure proper functioning.
- **Doing maintenance after hours** as not to interfere with staff work.
- **Handling the profiling** and adding of staff members.
- **Pricing, recommending, and ordering hardware.**
- **Keeping all software programs updated.**
- **Staying accessible** to handle staff's system problems directly.
- **Manage the day to day technology needs** behind the scene

"Part of our decision in going back to B4 Networks, was the ease of doing business with Bryan and his team"

"We have Full Confidence That B4 Networks Can Do It All"

FENA Insurance Solutions Inc.

"The service is always very good," Brenda says, "I have no complaints about the service whatsoever. They're always there, if we have something that's needed and we can schedule it - we schedule it. If it's something that needs to be done right away, they appreciate the fact that there's a reason for that, and they do their best to take care of it. Service levels are very good and the staff is very knowledgeable and very personable. Very easy to work with."

Canadian Broadband Declared a Service For All

Canadian regulators have declared broadband Internet access is an essential service everyone should have. Now they need to make it a reality.

Canada is now making a social policy shift that broadband Internet access is a fundamental tool everyone should have access to. And in that realization, the telecom regulatory agency in the country is also realizing that it can't do the job alone. Rather than just leaving high-speed broadband to market supply and demand forces, the regulatory community now wants to provide Internet access just as readily as phone service. And the two main players to provide that help would need to be the government as well as the Canadian telecom industry.

Broadband, explicitly defined by the Canadian Radio-television and Telecommunications Commission, or CRTC, now officially means providing Internet access that transfers data at a speed of at least 50 megabits per second to the recipient, and at least 10 Mbps from the sender. From a free market perspective, the country's citizens and the private market have already been doing an excellent job meeting this target. Specifically, approximately 80 percent of businesses and households are connected at speeds meeting the above minimum or higher. The CRTC wants the numbers to be at 90 percent by 2021 and 100 percent sometime between 2026 and 2030.

To make the above CRTC target a reality providers will be required to include an unlimited alternative in the broadband services they sell to the open market.

And mobile wireless service will be expected to be just as prevalent in households, at least to those communities adjacent to major transportation routes.

While regulatory agencies frequently end up at the opposite end of the table with industry, CRTC's sharpest critic, OpenMedia, was actually in full agreement when the Commission made clear its intent with broadband. And Rogers Inc. found no significant issues with the targets, stating they were quite doable. Rogers already delivers services at 20 times faster that CRTC's regulatory goal.

Of course, the devil is in the details, and the industry is well aware that CRTC's goals are very conceptual. The actual logistics of getting telecom service to remote locations is a very real challenge for many remote communities across the country. The industry expects that serious investment will be necessary, and it is willing to support a $750 million CAD fund to assist with infrastructure capital support. And the initial $100 million seed money will be from accounts originally intended for subsidized telephone services to isolated regions. The trade off to use these monies, however, is that providers then have to sell the broadband access at affordable flat rates of $25 a month.

The industry is not alone, however. The Canadian government has put $500 million CAD on the table as well for infrastructure investment. So there is now a very real groundswell to get service to 2 million additional customers nationwide. The persistence and initiative to stick to the plan depend on how well the CRTC can continue to policy support from all avenues.

Shiny New Gadget Of The Month:

WiFI Remote Cooking!

Ever wondered how you can make a moister, juicier steak, chicken breast, or pork chop? Tired of desperately trying not to overcook your food? Check out the Sous Vide Immersion cooker by Anova Culinary! This device is equipped with WiFi, allowing you to cook a perfect meal, remotely, on your time from anywhere.

Sous vide, French for under vacuum, is becoming increasingly popular with home chefs! All you do is vacuum seal your food with some herbs and spices, program your Anova with whatever temperature you want your end-result to have, and drop it in a water bath for a few hours.

Use steak for example. A perfect medium rare steak is roughly 134 degrees Fahrenheit. If your water is 134 degrees, the meat won't ever get hotter than that.

That means you *cant* overcook it!
You just give it a quick sear once you take it out, and you can enjoy a perfect steak. And since it's been vacuum sealed, the meat doesn't lose any of it's juices or nutrients! You can cook just about anything sous vide, from meats to vegetables, desserts, and even drinks.

Client Spotlight

KWIK MIX MATERIALS LIMITED

What We Do

For over 45 years Kwik Mix Materials has been manufacturing the absolute highest quality of pre-mixed concretes, mortars and related repair products. We also offer a variety of specialized services such as custom toll blending, custom packaging and small to large scale rotary kiln drying.

Who We Are

Informal, easy-going, unconventional, adaptable, most likely covered in cement,and teeming with "individuality". The last of which is open to interpretation... On a slightly different note: We are a close-nit variety of individuals that take pride in what we do, striving to produce strong, reliable and professional easy-to-use products. Our company philosophy is and has always been to enjoy what we do, treat people fairly, and make the best products on the market.

Why We Are Here

Well, to be frank, because the food industry has too many rules, and the alcohol industry is far too saturated. We are here because of the contributions of our employees, both past and present – Even a few that have been here since day one. This has allowed us to develop the current knowledge capital we have and need to gradually improve our products and functionality as a business.

Head Office:
KWIK MIX MATERIALS LIMITED
P.O. Box 520 Port Colborne, ON
L3K 5X7 Canada
Fax: 905-834-5160
E-mail address: sales@kwikmix.com
Toll Free Canada: 800-668-3140
US: 888-368-635

Southeastern Ontario
Planes Precast Concrete
P.O. Box 193 Kingston, ON
K7M 6R1 Canada
Telephone: 613-548-1864

kwikmix.com

Breached Companies

See Decline in Customers

Recent surveys indicate that most people will not do business with a company that has been breached. It is imperative to the success of your business to have the necessary security and processes in place to prevent being the victim of a serious cybercrime.

In the technology-based world, we live in today; data breaches are almost a daily occurrence. Not only are they a fiasco from a PR viewpoint; the breach is often invasive, and the company typically fails to respond appropriately as a result of the loss of revenue. Worse yet, once trust is broken, the company will then see a decline in customers.

While most people understand, there is always a risk when performing any task online, consumers expect that the business they are doing business with will protect their confidential information and keep it safeguarded. In fact, in a recent Gemalto global survey, the consensus was that customers do put the responsibility of the protection of their personal data with the companies that acquire it. Here are some other interesting findings from Gemalto from the 9,000 consumers surveyed:

Interesting Consumer Survey Results About Company Breach

- **30% of consumers believe that companies will protect their personal data**
- **58% of consumers are concerned about being a victim of a data breach**
- **21% of consumers have been affected by a financial data breach**
- **66% of consumers indicate they will not work with breached companies**

Now more than ever it is important to ensure that your business is safe and secure from cybercrime.

The Importance of Customer Trust

If you have any doubt about the effect a data breach will have on B4 Networks, consider these survey results and realize the majority of people would not do business with a company that has been breached. Now more than ever it is important to ensure that your business is safe and secure from these cyber crimes.

Customers need to know that the protection of their personal information is imperative to a business and that they have taken every precaution to ensure the safety of the data. Also, it is important for a company to show consumers exactly what steps they are taking to protect them to earn their confidence and trust. Surprisingly, most companies don't even realize that they are at such risk. In fact, they depend on marginally useful or outdated systems and actually think their customers are protected. This could be a serious issue for your St. Catharines, Welland, Niagara Falls, Grimsby and across the Niagara Peninsula business.

Do You Need a Breach Detection System to Protect Your Customers?

If you want to show customers that the protection of their private information is of utmost importance to your company, it is crucial to first educate them about the cyber security measures the company has taken. There are breach detection systems that offer protection for the valuable customer data. These security products make the company aware of potential threats promptly so they can take immediate action. Questions your business should ask include effectiveness, performance, system visibility, and time to detect threats.

Simple Closing Techniques for Smart People

Part Two, By Geoff Smart

Smart Closing Technique, Step 2

Let's say you're closing a deal and you've already taken the first step: you've summarized the client's underlying need...

Now you're ready for Step 2: Say what you plan to do.

Describe exactly what you'll do to help the client successfully satisfy their underlying need. Even smart people worry about putting themselves out there by offering a plan. They worry that someone may disagree with them. They worry about proposing a plan that doesn't work. That's why many advisors stay "safely vague" rather than offering a specific plan.

But being vague doesn't help leaders solve some of their biggest problems. You have to have the courage to propose a plan. For example: "I have some ideas about how you can achieve your goals. Want to hear them?"

"Yes!" (the client says, while taking out a notebook and a pen).

"There are five parts to what I think you need to do, in this order. They are designed to increase your power score, starting with priorities, who is on your team and relationships. First, there is no way you are going to be able to take the company in a whole new strategic direction without the board's support."

"That's true."

"**So first** we have to articulate your vision and your priorities on paper, with goals and strategy and budget implications, and then get the board's support."

"Right, it's going to change our budget, so rather than let the board nix it this fall, I should get out in front of this and get their support from the beginning."

"**Second**, you seem to have questions about the capabilities of many of the key leaders in the US, Europe and in your Asia region. It would be helpful to assess your team, to have a clear view of who is going to fit in the new organization, and who is not a fit."

"Yes, that would be helpful—to have an X-ray of the org chart and figure out who needs to go where to align with the new strategy."

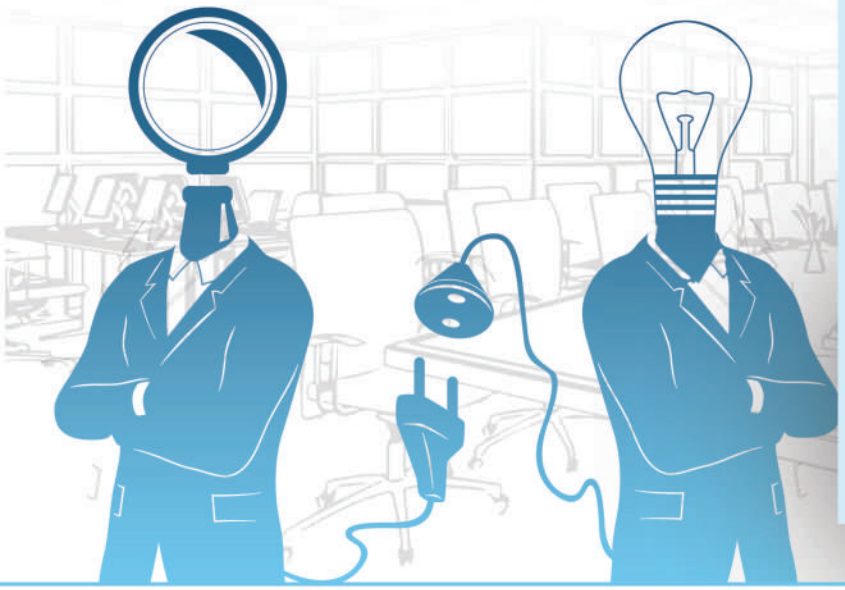
"**Third, fourth and fifth** will be all about culture change. Change the incentives. Change the meeting cadences of what metrics are tracked and discussed—who meets when to discuss what. And what some of our most successful clients have done in situations like this is design workshops—like a roadshow—for you and key leaders to educate and train the next two levels on what you expect from them, and why, in the new world order. This gets the troops aligned behind your new vision."

"Wow! Yes, yes and yes."

"And even if you do all of that, I only give it a 70% chance you will fully actualize your goal within three years—in the market and culturally. Still, that's a lot better than the 5% chance you give yourself today."

"I'd take 70% over 5%."

Now that you've stated your plan, you are in a much better position to close the deal.



About Geoff Smart

Chairman & Founder of ghSMART.

Geoff is co-author, with his colleague Randy Street, of the New York Times bestselling book Who: The A Method for Hiring and the author of the #1 Wall Street Journal bestseller Leadocracy: Hiring More Great Leaders (Like You) into Government. Geoff co-created the Topgrading brand of talent management. Geoff is the Founder of two 501c3 not-for-profit organizations. SMARTKids Leadership Program™ pro-vides 10 years of leadership tutoring and The Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a B.A. in Economics with Honors from North-western University, an M.A., and a Ph.D. in Psychology from Claremont Graduate University.

NEWS BRIEFS

Your phone may be spying on you, warns Edward Snowden.

While TV is a medium you watch, the Internet is a medium that watches you, as you watch... For example, intelligence agencies—or anyone else, for that matter—can run a nifty little piece of malware called "Nosey Smurf" on your phone to listen in on everything going on all around you. And it's not just phones. Internet-enabled devices—from Amazon's Echo to your new toaster—can have "ears," waiting for your command...or be used for more nefarious purposes. Snowden's warnings presaged last year's DDoS attack on DNS host Dyn that used connected devices like DVRs and even baby monitors to take down major sites like Twitter, Spotify and Amazon.

Forbes

This simple, 30-second breathing exercise wakes you up like a cup of coffee.

Whether you skip caffeine to get a better night's rest, or just wake up slowly, here's a quick way to activate your brain and give yourself an energy boost. It can help you beat that mid-afternoon slump, or to just get going in the morning. If you're doing it in the office, find a quiet place, like an unused corner or stairwell. Stand up straight, arms gently at your sides. Leaving your elbows pointing down, raise your hands up to shoulder level. Now, inhale deeply and raise your hands and arms straight up over your head. Quickly exhale and lower your arms. Repeat for 30 seconds, or until you're re-energized.

Lifehacker

No bigger than a water bottle when folded, this "personal drone" is packed with features.

DJI's new "pro-sumer" drone, the Mavic Pro, crams lots of excitement into its compact size. Unlike other, more confusing foldable drones, it's a snap to fold or unfold. Yet, at $999, including a light yet rugged remote, it's not just a toy. The Mavic Pro can climb at 16.4 feet per second up to 1,640 feet, and can fly as far as eight miles away at speeds up to 40 mph, though you'll start in newbie mode, at a top speed of 27 mph and max height of 400 feet. Its camera features obstacle detection and gesture recognition, and shoots 4K video, stored or streamed.

Mashable

Uh-oh...these AI machines just created their own secret language. And they're probably talking about us right now...

Well, sort of. And the last part is certainly not true. As far as we know... Google's AI team recently ran across something curious. Back in September, Google announced its Neural Machine Translation system had gone live. Using deep learning, it improves translation from one language to another. But the AI guys decided to take it a step further. Until then, they had to teach the machine how to translate. But having learned the process, could the machines then translate unfamiliar languages on their own? Turns out they can. So can they now talk among themselves? We don't know... Don't panic (yet), but do stay tuned.

TechCrunch.com

CYBERSECURITY MUST-DO CHECKLIST FOR BUSINESSES

Implementing and maintaining effective cybersecurity measures can be a daunting task, so start with the basics. Here are 8 things every business needs to do to stay protected.

1. Secure your office's internet with a firewall. If your office is wireless, make sure your connection is hidden to outside users and password protected.

2. Ensure there is an active antivirus software program installed on all systems.

3. Educate all employees about cyberthreats and how to avoid causing unintentional harm to your business.

4. Set stringent requirements for employee passwords, and change them on a regular basis.

5. Establish protocols for accessing and transmitting sensitive data.

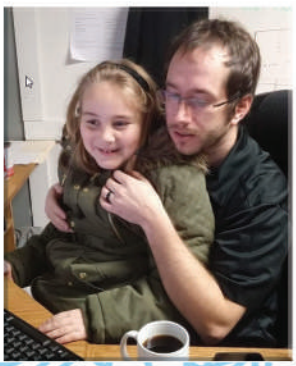
6. Put in place a backup system and disaster recovery plan for ALL files and data so that if your network or system becomes compromised, a copy of your files still exists.

7. Limit access to programs and data by ensuring that employee devices such as laptops, tablets, or mobile phones are password protected in case a device is stolen or misplaced.

8. Ensure your business' public website has adequate security to protect both your business and your clients from hackers and other cyberthreats.

Contact us at info@b4networks.ca or (905) 346-4966 to find out more about how we can help make sure you're secure against threats.

PHOTO ALBUM



TEKTIP

Never use the same password twice.

As we sign up for more and more accounts and services online it becomes extremely tempting to reuse the same password over and over again but this is extremely risky behavior.

If your login credentials are ever grabbed by a hacker – and with the number of data breaches in the news every week it's a case of when, not if – the attacker will have inadvertently gained access to your entire digital world.

If creating a large number of complex, hard to guess passwords is a challenge consider using a password manager such as LastPass (lastpasss.com) which can store all your credentials for you, leaving you with just one master password to remember.