

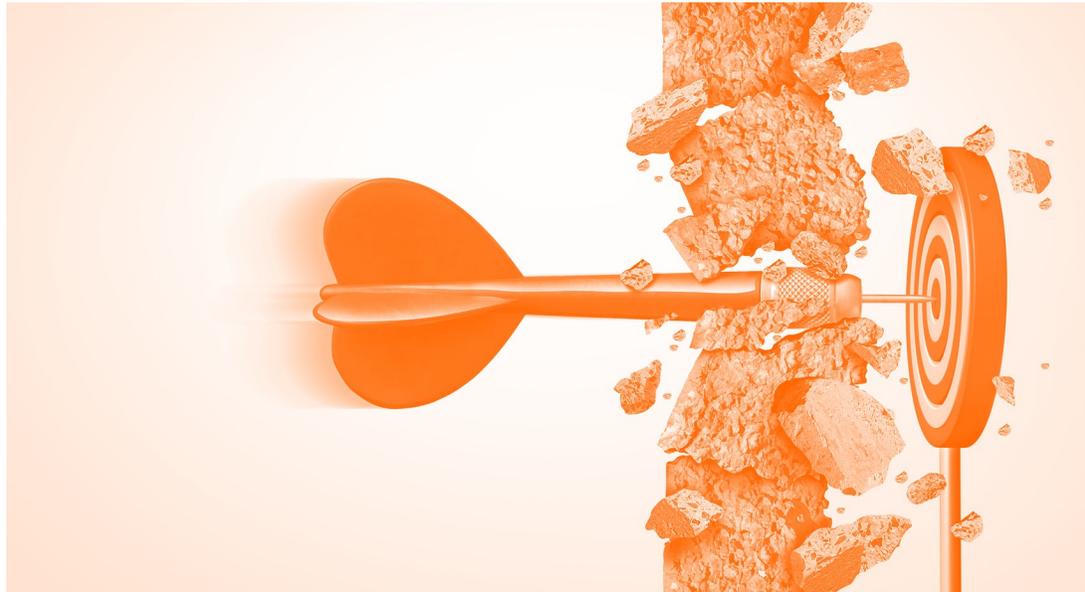
TECHNOLOGY TIMES

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

What's New

Interested in a FREE Dark Web scan for your company?

Contact us today! The FREE offer is good for the first 5 companies who contact us right away! Not one of the first 5 companies? No problem! You can get the Dark Web scan for your company for just \$49. Call the office right away at 701-364-2718 or email info@imsnetworking.com for more information!



Top 4 Ways Hackers Will Attack Your Network And They Are Targeting You RIGHT NOW

Most small and midsize business (SMB) owners exist in a bubble of blissful ignorance. They focus on the day-to-day operations of their organization, driving growth, facilitating hiring and guiding marketing, without a single thought given to the security of the computer networks these processes depend on. After all, they're just the little guy - why would hackers go to the trouble of penetrating their systems for the minuscule amount of data they store?

And eventually, often after years of smooth sailing through calm seas, they get hacked, fork out thousands of dollars to malicious hackers and collapse beneath the weight of their own shortsightedness.

The facts don't lie. According to Verizon's annual Data Breach

Investigations Report, a full 71% of cyber-attacks are aimed squarely at SMBs. And while it's unclear exactly how many of these attacks are actually successful, with the sad state of most small businesses' security protocols, it's a safe bet that a good chunk of the attacks make it through.

But why? As Tina Manzer writes for Educational Dealer, "Size becomes less of an issue than the security network ... While larger enterprises typically have more data to steal, small businesses have less secure networks." As a result, hackers can hook up automated strikes to lift data from thousands of small businesses at a time - the hit rate is that high.

Today, trusting the security of your company to your son-in-law, who assures you he "knows about

July 2018



This monthly publication provided courtesy of Rick Johnston, President of Information Management Systems

“Enabling People to Provide Great Products and Services - Anytime, Anyplace, Anywhere”

Want to Lock-in your IT Costs for the Next **THREE** Years? Sign up for IMS Total Care Services **TODAY!**

computers," isn't enough. It takes constant vigilance, professional attention and, most of all, knowledge. Start here with the four most common ways hackers infiltrate hapless small businesses.

1. PHISHING E-MAILS

An employee receives an e-mail directly from your company's billing company, urging them to fill out some "required" information before their paycheck can be finalized. Included in the very professional-looking e-mail is a link your employee needs to click to complete the process. But when they click the link, they aren't redirected anywhere. Instead, a host of vicious malware floods their system, spreading to the entirety of your business network within seconds, and locks everyone out of their most precious data. In return, the hackers want thousands of dollars or they'll delete everything.

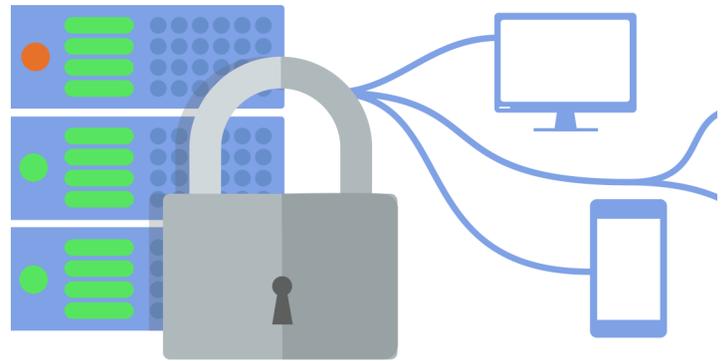
It's one of the oldest tricks in the hacker toolbox, but today it's easier than ever for an attacker to gather key information and make a phishing e-mail look exactly like every other run-of-the-mill e-mail you receive each day. Train your employees to recognize these sneaky tactics, and put in safeguards in case someone messes up and clicks the malicious link.

"...hackers can hook up automated strikes to lift data from thousands of small businesses at a time – the hit rate is that high."

2. BAD PASSWORDS

According to Inc.com contributing editor John Brandon, "With a \$300 graphics card, a hacker can run 420 billion simple, lowercase, eight-character password combinations a minute." What's more, he says, "80% of cyber-attacks involve weak passwords," yet despite this fact, "55% of people use one password for all logins."

As a manager, you should be bothered by these statistics. There's simply no excuse for using an easy-to-crack password, for you or your team. Instead, it's a good idea to make a password out of four random common words, splicing in a few special characters for good measure.



3. MALWARE

As described above, malware is often delivered through a shady phishing e-mail, but it's not the only way it can wreak havoc on your system. An infected website (such as those you visit when you misspell sites like Facebook.com, a technique called "typosquatting"), a USB drive loaded with viruses or even an application can bring vicious software into your world without you even realizing it. In the past, an antivirus software was all that you needed. These days, it's likely that you need a combination of software systems to combat these threats. These tools are not typically very expensive to put in place, especially considering the security holes they plug in your network.

4. SOCIAL ENGINEERING

As fallible as computers may be, they've got nothing on people. Sometimes hackers don't need to touch a keyboard at all to break through your defenses: they can simply masquerade as you to a support team in order to get the team to activate a password reset. It's easier than you think, and requires carefully watching what information you put on the Internet – don't put the answers to your security questions out there for all to see.

We've outlined some of the simplest ways to defend yourself against these shady techniques, but honestly, the best way is to bring on a company that constantly keeps your system updated with the most cutting-edge security and is ready at a moment's notice to protect you in a crisis. Hackers are going to come for you, but if you've done everything you can to prepare, your business will be safe.

Shiny New Gadget Of The Month:



Introducing The Snap SmartCam

Today, the security of your home is more important than ever before. Lawbreakers are constantly getting bolder, and as our technology advances, they switch up their tactics. With that in mind, all of us should be on the lookout for a security camera that's difficult to spot, is intelligent about the footage it collects, and grabs high-quality footage to identify burglars.

Enter the Snap SmartCam, a tiny little camera that looks – and operates – just like a phone charger. The innocuous-looking device uses motion-detecting technology to pick up when shady activity is going on in your house, and takes high-quality footage to catch a person in the act. If you're interested, the camera will cost you \$57.00 at the time of writing, a great deal for a security camera of any type, much less one that seems so useful.

Apple Users Are Getting Group Facetime

Apple's Legions of users love FaceTime, but there's a problem with the highly popular app. It only allows you to see and talk to one person at a time. Apple fans have been clamoring for Group FaceTime for almost as long as the app has existed, and soon, they'll get their wish.

Beginning with iOS 12, Group FaceTime will finally be "a thing," allowing you to simultaneously talk with up to 31 of your contacts. Even better, the new functionality will allow you to turn any iMessage group chat into a group FaceTime session, and switch back to iMessage at will.

Don't want to be on camera in a group setting? Apple has an answer for that too. The company has announced that when Group FaceTime is rolled out, you'll be able to place an Animoji over your face, or apply one of several different photo filters to disguise you. This is because they know that some days, you just might not feel "camera ready."

At the end of the day, Group FaceTime is probably going to be a lot like tabbed browsing was for many users. Until you try it, and until it's readily available, you won't truly appreciate its value. Once you try it for the first time, it won't be long before you're unable to imagine life without it. It's a cool, indispensable addition whose time has come.

Kudos to Apple's loyal fan base for keeping Group FaceTime on the radar, and kudos to Apple itself for finally listening to their customers and giving them what they want. While we could quibble that they took longer than we'd like to make this feature a reality, in the end, they listened. That is the essence of business, isn't it? Giving your customers what they want.



We received this article from our Blog on our website:
<https://www.imsnetworking.com/2018/06/12/apple-users-are-getting-group-facetime/>

Bits & Bytes

■ What To Do BEFORE You Go To Starbucks

You're in the car on the way home from Starbucks, basking in the glow of your triple-shot, low-foam, extra-hot pumpkin spice latte when you suddenly realize your laptop has gone missing. You drive back to the store like a caffeinated lunatic, only to discover no one has turned it in. What do you do?

Well, first you should notify your IT department (us!) immediately to tell them your device has gone missing. That way, we can change passwords and lock access to applications and data. We can also remotely wipe your device to make sure no one will be able to gain access — a key reason it's critical to back up your data on a daily basis.

Next, change ALL the passwords to every website you regularly log in to, starting with any sites that contain financial data or company data. If your laptop contained others' medical records, financial information, or other sensitive data (social security numbers, birthdays, etc.), you should contact a qualified attorney to understand what you may be required to do by law to notify the affected individuals.

An ounce of prevention is worth a pound of cure, so make sure you're engaging us to encrypt/back up your data and put remote monitoring software on all your mobile devices. Put a pin-code lock or password requirement in place to access your computer after 10 minutes of inactivity and smart phones after 1 minute. Make sure you get in the habit of logging out of websites when you're done using them.

■ Surefire Ways To Protect Yourself From Data Leaks, Hacks, And Scandals

1. Reconsider what you put online. This goes beyond social media posts. Even sharing your telephone number with a store associate can come back to bite you later.
2. Use password managers. This way, you can use different, randomized passwords for all your sites without losing track of them.
3. Use two-factor authentication. It's a no-brainer.
4. Encrypt the information on your drive. It's easier than it sounds!
5. Read privacy policies, otherwise you may be signing away more than you think.
6. Monitor your credit. That way, if someone tries to use your

info to make a big purchase, you can stop them in their tracks.

Inc.com, 4/26/18

■ Here's The One Reason Why You Need So Many Different Passwords...

Thinking up passwords and managing them is a big pain, no two ways around it. One website requires a symbol, and another requires 14 characters.

Meanwhile, your bank requires 10 characters, four PIN numbers and the answer to a secret question. In the midst of all this, it's easy to just use the same three or four passwords for everything — after all, that's more secure than a single password, right?

But imagine this. Say you use the same password for your Gmail, your Amazon and the account you use to order gift cards at a 10% discount for client gifts. One day, the gift card website is hacked. Not only do the crooks get your credit card info, they also get the list of all the website's users and those users' passwords. Then, they publish these freely on the internet.

But if you use different passwords for all your accounts, you're safe despite any crisis that may arise. Make sure you practice good password security.