The Tech chronicle

## What's New

Windows 7 reached its end of life on January 14th, 2020. A computer running Windows 7 will still continue to function, but if you continue to use it you leave yourself exposed. Microsoft no longer supports Windows 7 so fixing any problem you encounter will be more difficult and, more importantly, they are no longer pushing out security updates. Cyber attacks will become more targeted as weaknesses are exposed in Windows 7 and no further patches will be issued by Microsoft to correct these issues. If you still have Windows 7 machines at home or at the office we strongly encourage you to stop using these machines altogether and recycle and replace them with a Windows 10 machine or another secure alternative. If you have any questions about how to upgrade or replace these machines—give us a call, we'll be happy to help!

**February 2020**

This monthly publication provided courtesy of Craig Covington co-owner Canon Capital Technologies

### Our Mission

**To enhance our customers quality of life and the health of their business.**

# Top 3 Ways Hackers Will Attack Your Network — And They Are Targeting You Right Now

You might read the headline of this article and think, "That has to be an exaggeration." Unfortunately, it's not. Every single day, small businesses are targeted by cybercriminals. These criminals look for vulnerable victims, then attack.

This is the world we live in today. But why are small businesses the favorite target of hackers, scammers and other cybercriminals? It's simple—small businesses have a bad habit of NOT investing in cyber security.

Hackers have many methods they use to break into your network, steal data or put you in a position where you have to pay them money to get your data back. They use a combination of software and skill to make it happen. Here are three ways hackers and cybercriminals attack your network in an attempt to get what they want.

**1. THROUGH YOUR EMPLOYEES**

That's right, they'll use your own employees against you, and your employees might not even realize what's happening. Let's say a hacker gets ahold of your internal e-mail list, like the e-mails you have posted on your website or LinkedIn. All the hacker has to do is send an e-mail to everyone at your company disguised as a message addressed from you asking your employees for a gift card (an increasingly common scam). Another e-mail tactic is making a message look like it's from a fellow employee, asking everyone else to open an attached file, which is likely malware or ransomware. A third e-mail scam directs people to a phishing website, which is a website that scammers have designed to look

*Continued on pg.2*

*Continued from pg.1*

like popular websites in order to get login information to hack accounts. All it takes is a single click from any employee to let the bad guys into your business.

**2. THROUGH YOUR NETWORK DIRECTLY**

Some hackers aren't afraid of forced entry. Hackers and cybercriminals have access to black market tools and software that helps them get into networked devices – particularly *unprotected* networked devices.

For example, if you have a PC that's connected to the Internet and your network doesn't use any firewalls, data encryption or other network protection software, a hacker can break in and steal data from that PC and potentially other devices connected to that PC, such as portable hard drives. This method of entry isn't necessarily easy for hackers, but the effort can be worth it, especially if they can walk away with sensitive financial information.

**3. BY HOLDING YOUR DATA HOSTAGE**

Hackers are relying on ransomware more and more to get what they want. Hackers rely on e-mail, executable files and fraudulent web ads (such as banner ads and popups) to attack networks with ransomware. It goes back to the first point. All it takes is someone clicking a bad link or file and the next thing you know, you're locked out of your network.

This has happened to dozens of businesses and even city governments in the last year alone. The thing is that even if you pay the ransom, there is no guarantee the hacker will restore access. They can take the money and delete everything, leaving your business high and dry! This destroys businesses!

**"Hackers are just looking for easy targets and, sadly, a lot of small businesses fit the bill."**

All of these points are why you need to take a hard look at IT security solutions *and use them.* For instance, if you had all of your data *securely* backed up to the cloud and a hacker came in and tried to hold your data hostage, you wouldn't have to worry. They don't really have your data. You can tell them "no," then all you'd have to do is work with an IT team to get your network back up and running while scrubbing it of any malware or ransomware. Then, it would be a simple matter of restoring data from the cloud. Sure, you might be out of commission for a day or two, but in the grand scheme of things, it's *much* better than losing your business to these jokers.

Hackers are just looking for easy targets and, sadly, a lot of small businesses fit the bill. Just because you haven't had any major problems yet doesn't mean you won't in the future. The threats are out there and they're not going to go away. Invest in security, partner with an IT security firm and protect yourself. This is one investment that is truly worth it!

## Free Report: What Every Small Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems


This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

**Download your FREE copy today at www.ccmgtech.com/protect or call our office at (267) 381-2025**

# Three Simple Ways Introverts Leverage Their Strengths to Thrive in the Workplace

Most introverts can be drained by social interaction and stimulation. They need to recharge regularly, so days off are important in order for them to be at their most productive. If you are an introvert, here are three ways you can be at your best in the workplace:

- Manage energy more than your time. When you feel most energized, that's the right time to focus on creative work that requires more brainpower. Structure your days around your energy.
- Cultivate the right environment. Work in a space that calms you and energizes you. Set the right light (such as natural lighting) and invest in noise-canceling headphones.
- Say what needs to be said. Introverts constantly think but don't always speak up. Don't let communication fall to the wayside. Remember, we're all working together.

*Business Insider, Nov. 19, 2019*

# The First Mistake Bad Leaders Make In A New Job

The first mistake bad leaders make in a new job is subtle, common and avoidable: they come into an organization and they don't narrow the priority list.

In research for *Power Score*, we found that only 24% of leaders are good at prioritizing. And when a leader is bad at prioritizing, 90% of the time it's because they let too many priorities stay alive—in short, great leaders **prune priorities**.

What does priority pruning look like?

It looks like taking a weed whacker to the overgrown mass of useless priorities that grow inside organizations.

It looks like what Steve Jobs did when he returned to Apple and trimmed the number of products from hundreds to under 10.

It looks like what In-N-Out Burger (for those of you who have enjoyed this delicious West Coast treat) does in only giving you a menu of burger, fries and a drink.

It looks like what Scott Cook, founder of Intuit, did in making QuickBooks as easy as using your checkbook.

There are so many leaders I see who lack the analytical horsepower, the courage or the decisiveness to prune priorities, so they just let dozens, hundreds or even thousands of priorities live on in their organizations and distract people away from the small set of things that matter most.

If you want a simple way to prune priorities, use the one-page discussion guide straight out of our *Power Score* book. Have your team rate your priorities 1–10. If you are scoring a nine or 10, keep doing what you are doing. If you score less than a nine, then it's time to get out the weed whacker!

*Geoff Smart is chairman and founder of ghSMART. Geoff is the author of the No. 1* Wall Street Journal *best seller* Leadocracy: Hiring More Great Leaders (Like You) Into Government. *Geoff co-created the Topgrading brand of talent management and founded two 501(c)(3) not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring, and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a BA in Economics from Northwestern University, and an MA and PhD in Psychology from Claremont Graduate University.*