Technology Today

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"
Since 1984

Are your passwords for sale on the Dark Web?

The Dark Web is a hidden universe contained within the "Deep Web"- a sub-layer of the Internet that is hidden from conventional search engines. Search engines like Google, BING and Yahoo only search .04% of the indexed or "surface" Internet.

The other 99.96% of the Web consists of databases, private academic and government networks, and the Dark Web. The Dark Web is estimated at 550 times larger than the surface Web and growing. Because you can operate anonymously, the Dark Web holds a wealth of stolen data and illegal activity. *<continued on page 3>*

May 2018

This monthly publication provided courtesy of Ryan Haislar, Vice President of Computerease.

"As a business owner, 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!"

The World's Greatest Hacker Shares The Best Ways To Steal Your Company's Data


WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC) W721440021

NAME: MITNICK, KEVIN DAVID
AKS (S): MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: MALE
Race: WHITE
Place of Birth: VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: 5'11"
Weight: 190
Eyes: BLUE
Hair: BROWN
Skintone: LIGHT
Scars, Marks, Tattoos: NONE KNOWN

At a recent IT conference, I was listening to the "World's Greatest Hacker" share hacking methods that are 100% effective for getting access to a company's data. As the owner of an IT support company I was left wondering, do my clients and fellow business owners know the risks of these hacking strategies or that they even exist?

The presenter, Kevin Mitnick, who now works for the good guys as a cybersecurity consultant also shared his expert advice for IT companies like Computerease to help keep our clients protected. In this article I'll share a quick recap of his notorious past, some of the hacking techniques he used and also give you recommendations on how to keep your business safe.

Thankfully we already offer the recommended protections as cybersecurity services to our clients!

Becoming the FBI's Most Wanted Cybercriminal

As a teenager, Kevin Mitnick was always fascinated by how phone systems and computers worked. He played pranks on people by turning their home phones into pay phones, hacked a McDonalds drive-thru window speaker and even wrote a program to steal his high school computer teacher's password!

He never used his skills for criminal activity or personal gain, only to prove that he could do it. But, his exploits in hacking into several government organizations and over 40 major corporations still landed him on the FBI's most wanted list in 1995. Mitnick evaded the FBI for 3 years but was finally caught and sentenced to a prison term. The judge even sentenced Mitnick to 1 year in solitary confinement because the United States Government was afraid that he had the capability of hacking into the NORAD system and launching a nuclear missile from a regular pay phone!

Hacking For The "Good Guys"

Since his release, Mitnick now works as a cybersecurity consultant and is hired by government organizations and companies to try to hack into their systems and uncover vulnerabilities in their security. He has a 100% success rate in hacking into his client's systems and is quite famous with regular TV appearances, publishing multiple books and educating the public with live hacking demos.

Live Hacking Demo Of A Mac

Mitnick began his live hacking demo by saying, "If this happens to you, you will have a very bad day." He used a false Wi-Fi network to push a legitimate looking Adobe Flash update that gives him full control of a victim's *<continued Page 2>*

computer. He hacked into both a fully patched Windows 10 computer running McAfee Antivirus and a fully updated MacBook using this technique.

This technique gives hackers full access to all computer files, all the saved passwords for frequently visited websites and even a keylogger that can capture all of the credentials you enter with that computer. The hacker even has the capability of turning on the microphone and webcam of the infected computer!

The Dangers Of Social Engineering

A 1994 New York Times article titled Cyberspace's Most Wanted: Hacker Eludes FBI Pursuit contains an early mention of a very effective hacking strategy, "It is not clear if Mr. Mitnick has computing skills that are unusual in the world of programming, but he is clearly adept at what is known in the computer underground as "social engineering." A social engineering attack is when you try to manipulate a human target into doing something that allows you into their network or systems.

Mitnick gave the following examples of how people are very trusting and easily tricked into giving hackers access to critical business information.

Example 1: The CFO of a company is going on a trip or is at a golf tournament so the hacker gets the executive assistant's personal cell phone number. The hacker sends a spoofed text message that looks like it is coming from the CFO saying, "When Kevin calls go ahead and release the 3rd quarter financials to him, and by the way, please don't text me or call me because I'm on the golf course (or in a conference)." The hacker then calls the executive assistant who will send him confidential company information.

What is the chance that the executive assistant is going to follow through exactly as requested without contacting that person back? 95% chance!

The "World's Greatest Hacker" is actually a very nice guy! I'm personally very thankful that he works for the "good guys" now and shared some very critical cybersecurity advice that I will also share to educate my clients.

Example 2: Mitnick found the names of both the newest member of the IT department and the payroll administrator from LinkedIn for a large company that hired him to test their level of security.

He called the payroll administrator, pretending to be the newest IT employee and said, "We are changing how we access the payroll website so from now on visit this site instead. Go ahead and enter your credentials now to make sure that it works." Mitnick gave her the address of a FAKE website that looked exactly the same as the real website.

The payroll administrator gave her credentials AND access to all of the payroll information for the entire company to Mitnick after a single phone call.

Employees are very trusting of phone calls, texts and emails from people that they trust. Hackers exploit this trust and use social engineering to steal personal and company data.

How do you keep your business protected?

You can try to warn your employees to be skeptical and be careful of hackers and you can hope that it won't happen to you and your business.

Or, you can know that a trusted, local IT services provider will watch out for you by implementing the same recommendations as Kevin Mitnick shared for keeping your business safe. These include multi-layered cybersecurity protections, end-point cybersecurity software, email filtering and user education.

As your local St. Louis IT services company, Computerease offers all of these cybersecurity protections to our clients and to prospective clients. Call us today at (314) 432-1661 (MO) or (618) 346-8324 (IL) or email me at ryan@computer-service.com for a FREE Cybersecurity Risks Assessment ($297 value) to help keep your business protected!

Employee Cybersecurity Training

"95% Of Security Breaches Are Caused By Human Error"

Keep your client's data safe and secure. Don't be a victim!

One of your best defenses is to train your employees not to be fooled by sophisticated cyberattacks.

Get this essential training for FREE if you are a Computerease All Inclusive Client OR as little as $10 per person per year.

Visit www.computer-service.com/staysafe or call us at 314-432-1661 (MO) or 618-346-8324 (IL)

Are your passwords for sale on the Dark Web?

<*continued from page 1*>

Digital credentials such as usernames and passwords connect you and your employees to critical business applications, as well as online services. Unfortunately, criminals know this — and that's why digital credentials are among the most valuable assets found on the Dark Web.

The Dark Web is made up of digital communities that sit on top of the Internet, and while there are legitimate purposes to the Dark Web, it is estimated that over 50% of all sites on the Dark Web are used for criminal activities, including the disclosure and sale of digital credentials.

Far too often, companies that have had their credentials compromised and sold on the Dark Web don't know it until they have been informed by law enforcement — but by then, it's too late.

How can you tell if your business credentials are on the Dark Web?

Our 100% FREE and 100% confidential Exclusive CEO Dark Web Scan is your first line of defense. Simply fill out the form on this page with your name and company email address (yes, it has to be your company email), and we'll perform our Dark Web analysis.

Get more details about the Dark Web and get your FREE Dark Web Scan at:
www.computer-service.com/dark-web-scan
or call us at 314.432.1661 (MO) or 618.346.8324 (IL).

4 Steps To Finding Your Company's Diamonds In The Rough

Executives are always looking to inject "fresh blood" into their teams. They're on the hunt for shiny new talent to be that secret ingredient their organizations are missing. But in my numerous coaching sessions with entrepreneurs and leaders across the country, I found that an external search should usually not be the first step. Instead, I suggest that businesses look internally for hidden, untapped assets within the company. Here are four steps to start uncovering your diamonds in the rough.

1. DON'T HIRE TO FIT A TITLE.

It may be the way business has been done for half a century, but that doesn't mean it's right. You need to look at the individual strengths of each candidate and determine if he or she is right for your company and culture.

Make sure that you have a process in place to make hiring efficient. And as a part of that process, take time to identify those creative and out-of-the-box individuals you already have on your team. Ask pointed questions of everyone you consider for a given role, because this allows you to get a sense of how they think.

2. MINE FOR THE GEMS.

As you refine your hiring methods, you'll likely discover that the talent you're looking for might be right under your nose. Dig into your roster of existing team members. Create a company-wide survey for those interested in taking on creative or challenging initiatives, and give them the opportunity to be considered. The true innovators know what they can bring to the table, even if they're currently not in a role that's a perfect fit. If you give them the opportunity to shine, they'll come forward.

3. REFINE AND POLISH.

Once you've identified your gems, spend some additional time with them. Find out what inspires and motivates them. You may decide to modify your team member's role or transfer some responsibilities to others in order to better utilize your talented individual's strengths and unleash their creative prowess. Just make sure to set clear expectations with each person, explain why you're making the change and empower them to do what they do best.

4. FORMALIZE YOUR PROCESS TO FIND MORE GEMS.

This isn't a one-and-done process. It's important to meet regularly with people to find these hidden assets. Consider handing out surveys and holding brainstorming sessions regularly as part of your company culture. That way, new team members will come on board knowing there's an opportunity to shine in new ways, even if it's not what they were originally hired to do.

Focus on embracing and developing internal individuals with relevant skill sets before hiring. I guarantee there is a huge number of underutilized assets within your organization. Give them the space to shine brightly.

As the founder of Petra Coach, Andy Bailey can cut through organizational BS faster than a hot knife through butter, showing organizations the logjams thwarting their success and coaching them past the excuses we all use to avoid doing what needs to be done. Andy learned how to build great organizations by building a great business, which he started in college. It then grew into an Inc. 500 multimillion-dollar national company that he successfully sold and exited.

Master These 3 Roles To Become SUPER Successful

Everybody is eager to offer business owners free advice, but as a leader, your success will come down to how well you fill three key roles: leader, manager, and executor. First you need to lead. Start by accepting that any success or failure within your company lies squarely on your shoulders and that everything depends on your vision, strategy and understanding of your target demographic.

Then you need to manage. Surround yourself with people who are dedicated to making your business grow. Everyone should know the organization's goals and how you plan to achieve them. Transparency is vital to building trust and cohesion within your team.

Finally, you have to execute. Run through the individual steps on the path to your goal. Your employees should focus on the day-to-day tasks so you can cultivate the big-picture direction of your company. *Inc.com 2/21/18*

Ways Technology Can Make Your Business Meetings More Productive

Every entrepreneur knows how difficult it can be to run an efficient meeting. But most of them aren't leveraging new technologies designed to do just that. Rather than treating meeting participants like audience members, use a tool like GoWall to empower your team to contribute without disrupting your meeting's flow, keeping them engaged and on topic. Meanwhile, solutions like ParticiPoll equip any meeting with a poll that can provide useful feedback to implement at your next gathering. This is especially valuable for organizations that frequently host remote events, providing a quick breakdown of your meetings' strengths and weaknesses.

Speaking of remote contacts, Google Hangouts has made it easier than ever to set up video conferences where participants can move from chat to file sharing to video chat with no fuss whatsoever. And if you're unable to stand in front of your team with a whiteboard, consider implementing a whiteboard app like Cisco Spark Board, which uses shared screens to create a cohesive brainstorming session between you and your team. *SmallBusinessTrends.com 2/21/18*

Two-Factor What?

Two-factor authentication (2FA for short) is a system in which you must verify your identity in two separate ways to access an account. Sound confusing? It's not. Here's an example:

After enabling 2FA on a Gmail account, you have to enter your password each time you log in. Then you are asked to enter a six-digit code that you pull from your phone, a jump-drive-sized key fob or a program on your computer.

Only then do you have access to your account. That way, if someone steals your password, they still can't get in.

If you aren't currently using two-factor authentication with your most sensitive data and systems, look into whether it might be an option. The extra 15 seconds it takes to pull up that second code is laughably short compared to the time you'd spend dealing with a hacked account.

Who Else Wants To Win A Fun Prize?

The Grand Prize Winner of last month's Trivia Challenge Quiz is Cathy from Saint Louis, MO! She was the winner from the drawing of people who submitted answers for my quiz question from last month.

What was the name of the ransomware variant that infected millions of computers around the world in May of 2017?
a) Petya b) Wannacry c) Cryptoblocker d) Gremlin

The correct answer was b) Wannacry. Now, here's this month's trivia question. The winner will receive a $25 Ted Drewes gift card!

What was the name of the 1980's movie where teenagers unwittingly hacked into a military supercomputer?
a) WarGames b) Goonies c) Top Gun d) Terminator

Submit your response to answer@computer-service.com! Everyone who answers correctly will be placed in the drawing to win our fun prize!