TechTelegram
powered by neoRhino

4 Sneaky Tricks Cybercriminals Use To Hack Your Computer

December 2017

This monthly publication provided courtesy of David Pense, Network Engineer of neoRhino IT Solutions.

"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!"

There's no denying that cybercrime is on the rise. All it takes is a glance at a few big news stories from the past few years. Equifax exposed the information of over 100 million people, many of them not even users, to a surgical hacker attack. Last May, over 57,000 infections spread from a single ransomware source across 99 separate countries, with damage reaching everything from hospitals and businesses to vital public utilities like the German railway network. How many high-profile celebrities like Jennifer Lawrence have had their phone's picture feeds hacked and then dealt with the scandal of some maliciously leaked photographs, some of which they'd deleted years before?

But it's not just massive corporations or actresses that are being targeted day in and day out. It's small businesses, many equipped with far less robust security measures. In fact, if you're an entrepreneur, it's almost a statistical guarantee that hackers will target your business at some point down the road.

In your company's battle against cybercrime, it's essential to stay abreast of the rapidly shifting digital landscape. Only the most up-to-date security technology can even hope to protect you from the ever more sophisticated thieves pounding at your digital door.

However, it's also important to stay informed and vigilant. Here are 4 of the sneakiest and most common tricks thieves use to snatch your vital data:

Social Engineering Hacking. Though it can cost the victim thousands of dollars and do just as much damage as its digital counterparts, this trick doesn't require a single line of code. Instead, it exploits weaknesses in the "human network" of a business. For

Continued on pg.2

example: skilled scammers can call your business's cellphone provider, posing as the CEO's spouse, and convince the customer service rep to hand over passwords, Social Security numbers and sensitive personal information. Many IT departments are susceptible to this same scam.

Social engineering is also used to gather information that will later be used for a different strategy. Such as …

E-mail Phishing. This trick hijacks (or fabricates) an e-mail account with trusted authority and sends users an e-mail requesting they click a particular link. Maybe the e-mail looks like it's from the service department of your company's time-tracking software, seeking to remedy an error. When the link is clicked, however, ransomware or other malware spreads like wildfire through the system, and the user is at the mercy of the hackers. Usually, this is used to extort exorbitant sums of money from small businesses or individuals. Symantec reports that just last year, over 7,000 businesses of all sizes fell prey to some form of phishing scam, costing them more than $740 million in total.

> **"...if you're an entrepreneur, it's almost a statistical guarantee that hackers will target your business at some point down the road."**

Brute-Force Password Attacks Or Password Guessing. Either a hacker uses a software that, after putting in some data about the target (for example, the name of their dog or their anniversary), runs through potential keys ad infinitum. With sufficient information about the target, it's only a matter of time before the software breaks through.

More often than you might think, hackers can even simply guess the password. Infiltrators have common passwords that use real words or common structures memorized and can run through hundreds before giving up.

Fault Injection is a different story, usually only used by the most dedicated, sophisticated hackers around the world. Cyber thieves will use a complicated software to scan the source code of their internal software or network, noting every potential weak point in the system. Then, by splicing in strings of code, they can penetrate the system and steal data, inject a virus or cause other digital mischief.

How To Protect Yourself Against These Threats

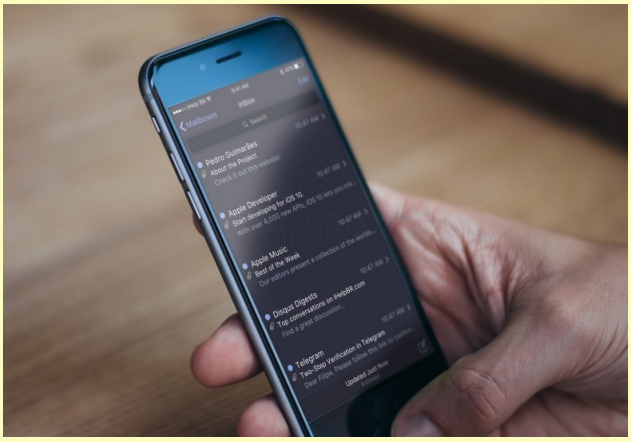
As they say, forewarned is forearmed, but it's not enough to keep your eye out for common hacker strategies. As the progress of technology marches on, so do the techniques and software used by hackers, resulting in an infinite number of permutations of ways they can penetrate your system.

The only way to be truly secure is by utilizing bleeding-edge security solutions to ensure you stay ahead of the breakneck developments in hacker technology.

Give us a call at (877) 85-RHINO and let us prevent your business from being a victim of sneaky hacker tricks.

rhynotel

VoIP Feature of the Month



Call Forwarding to Cell Phones

Call forwarding to cellphones can be incredibly useful for migrant workers, calls outside of office hours, and if you don't want to give out your cellphone number. You can even customize to send calls to your cell phones at set times of the day, the amount of time before forwarding, or to permanently relay for an extended period.

Want to learn more about Rhynotel's VoIP Systems and its features? Visit www.rhynotel.com or give us a call at (888) 661-6068.

Rhynotel, a neoRhino IT Solutions company.

Services We Offer:

- On-Site Help Desk Support
- On-Site Network Engineering including:
  - Cisco
  - Microsoft
  - Hyper-V & VmWare
- Disaster Recovery & Business Continuity
- Remote Managed Services
- Network Cabling
- Architecting and Implementing Enterprise Level Hardware Solutions

Give us a call today at 281-779-4850 to discuss your needs.

Free Report: If You Are Considering Cloud Computing For Your Company, DON'T, Until You Read This…

This report discusses in simple, non-technical terms the pros and cons of cloud computing, data security, how to choose a cloud provider, as well as three little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated.

Even if you aren't ready to move to the cloud yet, this report will give you the right information and questions to ask when the time comes.

Receive your FREE report today by sending us an e-mail at info@neorhino.com or call our office at (281) 779-4850.

3 Strategies For Dealing With Problematic Team Members

By Andy Bailey

You may have heard this common quote in business before: "If you can't change the people, change the people."

As a business coach, I'm accustomed to helping leaders and executives work through all sorts of issues. And the ones dealing with specific team members are the most common. Often, I find that even though a person may be causing specific challenges, managers want to avoid looking at the responsible party directly. But it's important to understand that changing the people is a necessary act for any successful organization. After all, while training can improve performance, it's difficult to change attitudes.

Below are three tips to improve the talent management and procurement process to train fruitful, challenge-free team members who will grow into leaders.

1 Avoid Stray Dogs

If you've ever hired any team members who turned into poorly performing players (and who hasn't?), your first step should be to rethink your criteria.

"Stray dogs" are those hires who don't fit much of an organization's criteria but end up getting picked anyway. To set up your talent management processes the right way, develop a process of ensuring candidates meet your criteria and steer clear of those stray dogs.

2 Trust Your Gut

Leaders are often too focused on the details in a resume and let that override their gut feelings. It might seem like a smart decision to rely on facts and figures that a candidate presents, but you can't fully know the circumstances surrounding those victories. Sometimes, it's best to rely on your sense of how a potential hire will perform. If there's any doubt, move on until one feels right.

3 Triple Your Time

Finding the right people becomes more difficult when there's a time crunch. To thoroughly vet potential hires, leaders need to start early by devoting a sufficient amount of time to the hiring process. Before getting started, identify efficiencies you can make during the hiring process. Vet candidates *before* you need them, not after.

As the founder of Petra Coach, Andy Bailey can cut through organizational B.S. 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.

Send Your E-mails At These Times Any good salesperson, marketer, or client communication specialist worth their salt spends a lot of time carefully constructing e-mails, from the perfect subject line to the ideal sign-off. But even the most savvy senders often overlook one of the most important parts of the process: the time of day you send your e-mails out. Research from MailChimp and HubSpot shows that emails that arrive between 9:00 a.m. and 11:00 a.m. (in the recipient's time zone) are much more likely to get read than their later counterparts. Day of the week, however, doesn't really matter. As long as it's a weekday, the open rate should stay consistent.
- *Inc.com 9/19/2017*

4 Ways Technology Can Improve Your Business Many small-business owners struggle with staying up-to- date on technological trends. Statistically, your company is probably behind the times. Studies show that only about a third of small businesses even have a website, and those that do haven't optimized them for mobile devices — an absolute must in the contemporary marketplace.

The same goes with a Facebook page. Every business, no matter how old-school, should have at least the minimum of a social media presence, and those that really want to succeed should amp up their online activity with YouTube videos and a Twitter feed. Marketing can't be limited to one-and-done flyers you send out once a month anymore. Instead, you need to fire on all cylinders, allowing people to easily search for and find your business online. This means adequate search engine optimization and syncing your offers up between digital advertising avenues.
- *RDSDigitalMedia.ca 9/8/2017*

Does Your Business Need Data Breach Insurance? In the past few years, data breaches into small businesses by malicious hackers have climbed to an all-time high. According to data compiled by the Identity Theft Resource Center, at least 1,093 data breaches occurred in 2016, 40% more than the previous year. And this trend shows no sign of slowing down. In response to rampant cyber-attacks across the country, many small businesses have turned to data breach insurance, designed to financially protect and support victims of malicious hacking. If your system becomes infected by ransomware, the insurance can cover the cost and guide you through the process so you can mitigate damage and stress.

If your business creates and stores vast quantities of sensitive data — especially if that data is a vital asset to the company — you should at least consider protecting yourself with data breach insurance. When all else fails, it can mean the difference between shutting down for good and staying afloat in the midst of crisis.
- *SmallBizTrends.com 9/5/2017*

Thank you for reading! See you next month!

neoRhino IT SOLUTIONS