smart office CONNECT

October 2016
Tech News and Information

pcWorks plus
Professional Solutions

Month Focus

This months focus is on your back up system. Some of you may have already received a letter to let you know that your current back up system is end of life.

We do not expect our customers to "Keep up with the Jones", but we want to make sure that as technology changes and the hackers become smarter, we are making our customers less venerable to attacks and data loss.

Consider these questions:

⇒ What data do you have and where is it saved?
⇒ What is your tolerance for down time? 4hrs, 1 day or 1 week?
⇒ What is your plan for a true disaster? Fire, theft, water?
⇒ What processes, like payroll, are critical to keeping your business run?

If you would like a more in-depth dive into your back up and storage, contact us today.

814-742-9750
sales@pcworksplus.com
www.pcworksplus.com

The One Attack No Tech Can Stop

You can defend your data with all the latest and best technology. But if just one team member gets tricked into giving away the keys to the castle, it's game over. Hackers know this. And that's why so many use social engineering to break in.

And it's not just the big companies you hear about on the news. On February 3, 2016 a suspect posing as the CEO of Magnolia Health Corp. obtained a spreadsheet with sensitive data about their employees. On February 23, someone posing as an employee of Central Concrete Supply Company obtained confidential W2 records and disappeared with them.

In a 2011 survey, Check Point Software Technologies found that nearly half of the companies surveyed reported one or more social engineering attacks resulting in losses ranging anywhere from $25,000 to $100,000 per occurrence.

Unfortunately, there just aren't any whiz-bang tricks or tools that will automatically prevent a clever "social engineer" (SE) from breaking in. The keys to protection are awareness and vigilance. To help you know what to watch for, here are five common ploys - and how to deflect them:

Familiarity - In this type of scheme, the hacker becomes familiar to an employee. Social networking sites can reveal an employee's schedule and favorite hangouts. The hacker might then frequent the same bar or restaurant. After a drink or two, some key fact may slip out... The best way to bust this ploy is to be careful to not get lulled into a false sense of security around people you haven't thoroughly vetted.

The Consultant - A social engineer poses as a consultant for

Continued pg.2

hire. Once they get the gig they can scoop up all the info they need from you and your team because of their seeming authority. Watch for this especially with IT consultants. Do NOT trust blindly. Vet every consultant, and never give all the keys to the kingdom. Just because someone has the skills to fix your server or network doesn't mean they won't steal your data. Vet thoroughly, and, as Ronald Reagan said, 'trust but verify'.

"When you see this exploit unfolding, call security."

Piggybacking - The SE waits by a secured door for someone to use their passcode and enters right behind them. Or the SE struggles with a heavy box and asks a legit employee to hold the door open for them. Being kind and helpful, the employee helps the SE right into the building… free to do as they please. To foil this one, never forget the dangers of allowing a stranger in without proper clearance.

The Interview - Key information often escapes during interviews. A smart social engineer will gain an interview and deftly pick up all the information they need to hack into your network. Make sure any data provided during an interview offers nothing in the way of secrets. Keep the conversation light, or even superficial to avoid leaking critical data.

Angry Man - You may have seen this on TV… Somebody has an angry tone on the phone, or is grumbling to themselves as if they've just had an argument. We all tend to avoid people like that. Enough people avoid them and the way is cleared into the heart of the company - and your data. Don't go along with it. When you see this exploit unfolding, call security.

The key to preventing social engineering attacks is a well-trained workforce. You and your people may be your company's greatest asset. Yet without regular, proper training, human beings can be the weakest link in your company's data defenses.

Here's how to protect your network from a costly cyber attack

To learn more, please go to www.pcworksplus.com/reports . Download this report: *The Top 10 Ways Hackers Get Around Your Firewall And Anti-Virus To Rob You Blind* steps you through 10 ways to protect your company from the coming deluge of cyber attacks we can expect over the next several years and beyond.

Call today at 815-742-9750 or email sales@pcworksplus.com for more information on how to make sure your network is secure.

Miss the last couple months of Newsletters with important tech information from PC Works Plus?

Check out the archive of past newsletters.

http://www.pcworksplus.com/tech-tips-tricks-and-industry-news/newsletter-archive/