VOLUME 4, ISSUE 12 DECEMBER 2021

MTC TECH TALK

For Humans Not Geeks!

Your resource for the latest technology updates and opportunities for your success.

Hacker Tips:

The Top 5 Tricks Used to Hack Your Computer Network

What's In This Issue?

Meeting Tree Computer
☎ (845) 237-2117

The contemporary world is rife with digital thieves. They're penetrating the complicated data structures of huge credit-monitoring companies like Equifax, scooping up the personal information of millions of people. They're releasing sensitive customer data to the public from discreet businesses like Ashley Madison and T-Mobile. They're watching webcam feeds of our celebrities without them knowing; they're locking down the systems of public utilities like Colonial; they're even managing to steal thousands of gigabytes of information directly from high-profile government entities like the CIA.

While these stories all make the news, they're also targeting small businesses just like your own and extorting them for thousands and thousands of dollars.

When running a company, it's vital to have a dedicated security team equipped with the most up-to-the-minute security technology on your side to protect you from these malicious cyber threats. But it's not enough to just leave it to somebody else. You have to be up to date on the threats facing your company.

Here are five of the most common ways hackers infiltrate your network:

1. Phishing Scams

Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment.

An excellent example of a phishing scam is the "deactivation scare." It's a lure that often works because nothing scares people more than a deactivation notice claiming your account will be deactivated if you don't follow a convenient link, enter your username and password and take immediate action – probably to update your credit card.

It's easy to ignore these phishes if you don't have an account with the company they claim to represent. But if you do have an account, it's easy to fall for this trick.

2. Social Engineering

Social engineering is a type of "hacking" that uses real people to carry out its schemes rather than intricate lines of code as used in a phishing email. It is usually part of a more significant "con" intending to get the victims to give up usernames or passwords, send money or gift cards, or install malicious software on their devices.

For example, instead of sending a phishing email, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his/her password, information that will then be used in a future attack.

3. Password Hacking

You may think that your passwords are clever and complicated, filled with exclamation points and random numbers, but it's rarely enough. With information gathered carefully from social engineering or a simple check of your social media accounts, hackers use brute-force attacks to figure out that your password is the family dog's name, followed by your anniversary (for example).

A brute force attack involves 'guessing' usernames and passwords to gain unauthorized access to a system. While some attackers still perform brute force attacks manually, today, almost all brute force attacks are performed by bots. Attackers have lists of commonly used credentials, or real user credentials, obtained via security breaches or the dark web. Bots systematically attack websites, try these lists of credentials, and notify the attacker when they gain access.

4. Fault Injection

Sophisticated hackers scan your business's network or software source code for weak points. Once they locate its weak spots, they will surgically attempt to crash the system by sending through snippets of code created expressly for that purpose. Different commands will do different things, whether they want to deliver a devastating virus, redirect links on your website to malicious Malware or steal and erase vast swathes of information.

5. USB-based Malware Infections

It's possible to come across both unintentional and intentional infections. Unintentional infection might occur when someone plugs an unprotected USB into a poorly safeguarded system in an internet café, an airport, or anywhere with poor public endpoint security (which is about 70% of places). It seems harmless to use this USB to transfer information back to your machine at the office, but you'd be taking a rather substantial risk. The effects of which you may not detect until days or weeks later, and there's no telling what damage has already been done.

Or, at the last conference you attended, someone handed out free branded USB sticks to keep their business top-of-mind. Unfortunately, hackers will sometimes covertly slip a bunch of infected USB sticks into a company's stash. The instant somebody tries to use one, their computer is taken over by ransomware.

So What Can You Do About It?

It's a scary world out there, with virtually everyone left vulnerable to digital attacks. However, knowing the strategies hackers deploy is half the battle. Technological solutions can help rebuff attempts to take advantage of your staff. Still, the best solution is to provide ongoing awareness training and teach your staff to be more skeptical. Remember, this is not just about clicking on links.

Your Tech Tip of the Month

What is Least Privilege (PoLP) and Why Is It Important.

Remember the Home Depot and Target data breaches? Hackers walked away with millions of debit and credit cards, and email addresses. The payment card information was later sold on the Dark Web. The email information made millions of consumers vulnerable to phishing scams.

This month's tech tip shows how an ounce of prevention could have been a pound of cure:
https://www.meetingtreecomputer.com/tech-tip-70-all-you-need-to-know-about-least-privilege/

How Flexible is Your Technology Budget?

We've all become a lot more flexible in business over the past couple of years. We've had no choice, right??? But while you and your team have gotten used to different working arrangements, has that flexibility moved over to your budget?

As you create your IT budget for 2022 you may fall into the trap of trying to keep your expenses low. But the sad fact is that, whether budgeted for or not, a ransomware attack or another critical incidents will cost you a lot of money. And as you may know, cyber-attacks are rising at a rapid rate, this year we've seen some of the most significant incidents ever.

It's crucial for you to do whatever you can to avoid an attack on your business. But also, to plan for what happens if you are attacked.

If you're working with an IT support partner, it's a good idea to get them involved in your IT budgeting. They'll be able to give you an expert view on the right things to consider and include in your plan. Talk to us if you need help.

Uh-Oh... Virtually All Businesses Have Been Affected By This. Has Yours?

A report recently found that a massive 98% of all businesses have experienced at least one breach of their data stored in the cloud, over the past 18 months.

What?

That's almost ALL businesses.

Has yours been affected? A breach could be something as small as an employee losing a device that's still logged into a cloud account... right up to a hacker getting full access to your data.

This is why every business should prepare an incident response checklist. It's your way of preparing a head of time what you'll do when a problem happens. It will help you minimize damage and recover from any breach more quickly.

Here are several things that must go in your plan:

Key people: Who will be responsible for actioning the plan? Which people will play crucial roles once the plan has been triggered?

Internal communication: Keep a list of everyone who needs to be notified, as well as details of how their job will be impacted

Alternative communication methods: If your email or VoIP goes down, how will you let your clients know that there may be a service impact?

Document: Record all of the details of the issue, and the actions your people have to take.

Can we help you think through all the implications and pull together your plan?

Would Your Business Survive the 4 Beer Test This Holiday Season?

Whether you'll be having a traditional office Christmas party this year or not, I'm sure at least some of your team will find a way to celebrate together over a few beers after work one day.

And that's why it's worth asking if your business can pass the 4-beer test.

What's that?

Well, we figure 4 beers is about the stage where people start to "relax" so much, they start to forget the important stuff.

Like picking up their laptop bag when they leave the bar. Or as they're jumping off the train home in a fluster, after a little impromptu nap ...

Laptops and cell phones get left in bars and on trains all the time, especially on dark winter nights like these.

The thing is – depending on your IT setup, a lost laptop can either be a minor inconvenience. Or a complete disaster.

How can you tell which?

Ask yourself these 3 questions:
- Is it encrypted?
- Is it password protected?
- Can the data be wiped remotely?

If it's a "yes" to all three, you can relax. It's annoying you've lost your device... but your business's data is safe. No-one can access it.

If you can't answer all three questions with a resounding "YES" ... uh-oh... problem. These days, the loss of data is a much bigger deal than the loss of a device.

If you're not 100% sure you can answer all 3 questions with a big fat YES... then give us a call. We can check for you.

I've heard I can voice type on websites. Is that true?

Yes, if you're using Microsoft Edge in Windows 10 or 11. Turn it on by pressing the Windows logo key + H.

How do I schedule appointments in email?

In Outlook you can select Reply with Meeting in the Ribbon. This creates a new meeting request, with your email in the body of the meeting request.

I deal with clients in different countries. Is there an easy way to deal with time zones?

You can add multiple time zones in your Outlook calendar. Go to File > Options, click the Calendar tab, and Time zones, tick 'Show a different time zone' and give it a name. Repeat as necessary.

Submit Your Question Here:

mduci@meetingtreecomputer.com

This is how you can get in touch with us:

call: 845-237-2117 | email: info@meetingtreecomputer.com
website: www.meetingtreecomputer.com

Follow Us