April 2022

TechTidbit.com

brought to you by Tech Experts

Grow Your Business With Influencer Marketing

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Traditional influencer marketing means relying on celebrities and famous bloggers to generate traction about your brand. However, as time changes with the boom of social media, the number of influencers in the market is rising.

The influencer marketing technique involves affiliating with famous social media celebrities and bloggers for the purpose of promoting product or services to their followers.

While collaborating with influencers, identify their audience reach and engagement. This marketing tool's main purpose is to drive sales and build your brand's credibility.

Campaign surrounding KPIs

Influencer campaigns are exciting and attractive because of numerous ideas and sparks in the campaigns.

You can increase your brand's growth through interesting methods with the help of influencers. Before starting an influencer campaign, identify a goal and target to evaluate the outcome. When you understand the purpose for an influencer campaign, you can draw a line between what works and what doesn't for future marketing drives.

For setting goals, choose KPIs (key performance indicators) corresponding to your business goals. KPIs will enhance your focus to achieve the target. You need to depend on specific goals for campaign success.

Finding the influencers

While selecting influencers, you cannot simply rely on their popularity among the audience. The relevancy of the influencer with the brand is the essence of the marketing campaign.

Before you start your search for influencers, check your support to find someone already aware of your brand. Besides allowing easier communication about the campaign, they will receptively work with your brand as well. Furthermore, with these influencers, you increase your growth rate drastically.

Clear and concise outreach

Communicating your idea for a collaboration with the influencer should be the easiest way.

Many businesses do not receive proper responses from influencers because they fail to communicate through proper channels. The mailbox of these influencers is overflowing with fans and supporters. Furthermore, they receive numerous offers for collaboration. You need to give them a reason to choose you instead of others. Here are some tips that you should follow:

- Add an attractive subject line
- Mention why you are credible
- Share some solid reasons why they are perfect for your campaign
- Explain what benefits they will receive after collaboration
- Your proposal should be sweet- and short

Collaborating with the content

Share your idea with influencers and seek their suggestions. Remember, you are collaborating with an influencer rather than hiring them.

Influencers should feel freedom in sharing their ideas because they know about grabbing the attention of their audience. Explain your goals to them, and they might come up with a creative idea for the campaign's success.

Choosing the platforms

Initially, Facebook's marketing strategies were amazing to deliver ROI for the businesses. As the audience's interest increases, you can choose from various platforms as a means to grab their attention. Moreover, new ideas and tools are available to help achieve business goals.

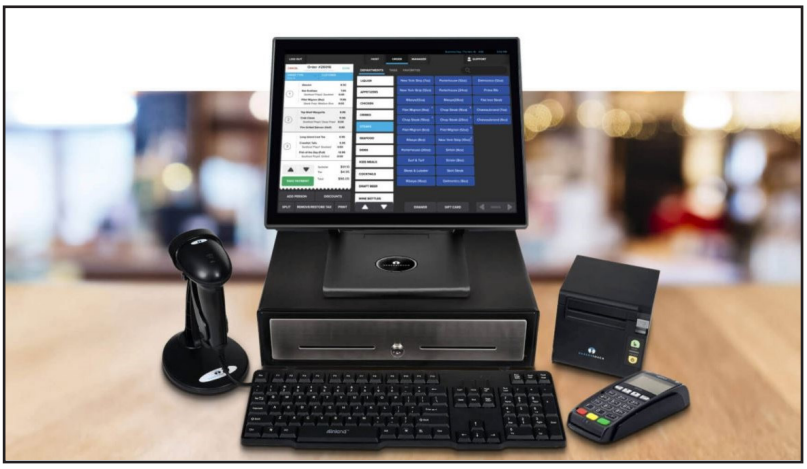
As competition on popular platforms grow, you should leverage influencers on platforms such as Snapchat and TikTok. Digital marketing is shifting drastically as social media platforms give rise to new and innovative marketing techniques.

For setting goals, choose KPIs (key performance indicators) corresponding to your business goals. KPIs will enhance your focus to achieve the target. You need to depend on specific goals for campaign success.

How To Choose The Best POS System For Your Business

"While selecting a point of sale system, you need to consider various factors, including your business type. For instance, if you have a restaurant, your business process will be different than a retail business. Therefore, you need to choose a system specific to your business needs."

A good POS system will not only help you manage the transaction, it also enhances your cash flow system. With these two factors in play, you can easily grow your business.



By implementing an advanced POS system, you can provide numerous payment options to your customers. These options include online payments, card payments, and cash payments. Furthermore, it also simplifies your business. An effective all-in-one point-of-sale system will help you efficiently perform administrative tasks.

While selecting a point of sale system, you need to consider various factors, including your business type. For instance, if you have a restaurant, your business process will be different than a retail business. Therefore, you need to choose a system specific to your business needs.

How to Choose a POS System: Identify your needs

First, you need to understand your business requirements. Your goal is to find the best solutions to your problems. However, you cannot make a better decision without identifying and considering your problems. Therefore, you need to ask some questions. The answers to these questions will lead you to pick the right solution:

- What type of product do you sell?
- How do you accept the payments?
- How many people do you have on your team?
- What payment method do your customers prefer?
- How will you interact with your audience?
- What type of solution are you currently using?

Perform market research

After answering all the above questions, you can use a search engine to list down the best options according to your needs. However, with so many options, you might feel overwhelmed. Below, you will find some best tips that will lead you in the right direction:

- Check the system that your competitors are using.
- Communicate with the POS system provider and seek help from professionals
- Visit tech websites

Check the features of service providers

After shortlisting your options and narrowing it to two to three POS systems, you can investigate the services they are offering. Here are some factors that you should consider while evaluating your options:

- What features are they offering?
- How will their system work for your business?
- What is the price of the tool?

Download the trial version

Once you complete your research about the best POS system for your system, you should download and install the trial version. When you perform the actions on a trial version, you can understand if this tool will benefit your business or not and how well it fits your company.

Why Protecting Your Printers From Cybercrime Is A Must (And Eight Tips For Improving Printer Security)

Printing devices are often overlooked when it comes to security. But the reality is, cybercriminals can hack your printer to get confidential information. Your printer is probably the last piece of computer equipment you thought needed protection from cybercriminals. But the truth is very different.

Attackers actively try to locate the weakest links in security to gain access to and exploit valuable data. And among the weakest links is the printer.

Printers have access to your devices, network, and the Internet. This new open-access functionality makes them an ideal target for cyberattacks.

Unfortunately, many business owners overlook the importance of securing their printers and mainly focus on computers and mobile phones.

Most people still perceive printers as internal devices that serve basic functions. For this very reason, they are an easy target for cybercriminals.

Other than performing unauthorized print jobs, hackers can access confidential information as well as all connected computers and networks all through a printer.

You may also not be aware of the amount of valuable data your printer can store about you – tax files, bank details, financial records, employee information, personal information, etc. All a hacker needs to do is get into the operating system of your printer, and they can collect this sensitive data.

If you've just realized the importance of securing your printer, keep reading. This article shares eight tips to help you do just that.

Tip #1. Make Sure Your Printers Are Configured Correctly

Many things can make a printer vulnerable to cyber threats and security breaches. So, you want to get the basics

right to ensure the attacks don't happen to you. To start with, make sure to change the default password on your printer. Since anyone can access a printer remotely, a simple "123456" code won't suffice.

Second, make sure you're using your own router to print files remotely. Never connect to "Guest" networks.

Tip #2. Inspect Print Trays Regularly

This one is a no-brainer, but everyone could use it as a reminder. Make sure to check your print trays and get rid of unused pages carrying sensitive information. There's no easier way to prevent data leaks than this.

Alternatively, you can get a shredder for your office and shred the papers you don't want anyone to see.

Tip #3. Install Malware and Firmware Updates

Invest time and effort to ensure that your malware and firmware protection are up to date and can handle all types of hacks.

The good news is that many printers come with pre-built malware protection.

HP, for example, installs the HP "SureStart" software in their printers that monitors approaching targets when the printer is on. The software can shut down the device if an attack comes its way. This is a great way to prevent attacks from spreading further within the network.

Tip #4. Limit Access to the Network

Unprotected printers in a network are an extremely easy target for cybercriminals. Sure, businesses and offices require printers to access networks to perform remote prints. But if you can do the job by disabling the network access, make sure you do that.

If not, tweak the printer and network settings to only allow the device to take print jobs from the network you trust. This will help avoid outside interference and security breaches.

Tip #5. Update Your Printers

Updating a printer is equally as important as updating your phone to the latest software. Much in the way iOS developers look for bugs and fix them in a new update, printer manufacturers work toward known device vulnerabilities and update the software for added protection.

Look for printer updates so you can easily overcome known threats to the printer. Ideally, update your printers every quarter to get the most out of the security benefits.

Tip #6. Install a Firewall

If you run an office, chances are you already have a firewall. But in case you missed this requirement, now's the time to do it.

Using a reliable firewall helps keep printers safe from cybercriminals. Your computers most likely come with pre-built firewalls, and all you need to do is keep them enabled. But there are also specialized firewalls for homes and offices that offer advanced security and make it virtually impossible for anyone to break in.

Tip #7. Encrypt Your Storage

Printers with shared networks can perform distance printing. And when a print job is in transit and travels from a computer to a printer, hackers can intercept the data and exploit it.

To keep this from happening, encrypt your print jobs. Also, make sure the sensitive data on your printer's hard or internal drive is encrypted as well.

Keep in mind that when you print a document, that file is often stored as an image within the printer and makes it an easy target for hackers. It's why you should use an encryption tool to protect your data. Luckily, many modern printers have this tool pre-built.

Tip #8. Educate Your Employees

If you work in an office, chances are you aren't the only person using the printer. Everyone that has access to it needs to be aware of the responsibilities that come with its usage. Make sure to talk to your employees about ways to ensure both the physical and virtual safety of the printers.

Your staff should also be careful when using their mobile devices to print, as smartphones are easier to hack than standard computers. Explain to them what phishing scams are and how they can avoid being the victim.

Finally, make sure it's clear to them how they can use confidential information in your company.

Whether you use printers in your office or at home, take a moment to see how you can enhance its security before your next printing job.

Which Type of Hacker Is Endangering Your Business Data?

Your data is pivotal to running a successful company. If you don't have proper security measures in place, hackers can easily steal your data and take you out of business. Cybercriminals might be the biggest threat facing your company. Besides gaining access to your money and accounts, they can also take over critical software, preventing you from collaborating with clients.

Any organization can fall victim to hacking. However, small and medium businesses are particularly at risk. Why?

Too often, their owners don't always address cybersecurity when launching their company. Sometimes, they even just hire the first IT service provider they see. They also don't know how to shield themselves from online attackers, making them low-risk targets.

As a result, these organizations often go under due to the loss of sensitive data. It isn't a risk you can take.

The 5 types of hackers to watch out for

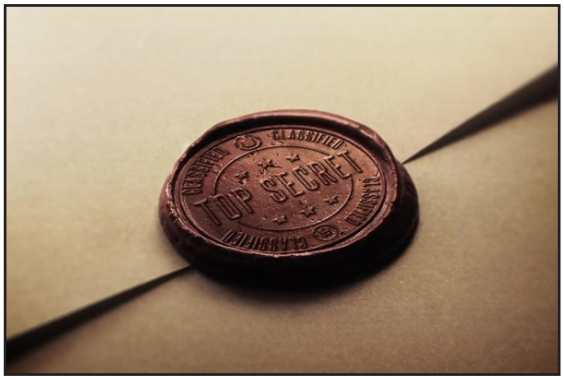
Here's a quick list of potential hackers, depending on what they're after:

#1. Hackers Who Are After Personal Information. Many hackers are dying to get their hands on the personal information of your clients and employees. It includes birth dates, financial data, and social security numbers.

Social security numbers might be the most valuable asset they want to get ahold of since cybercriminals can use them for various purposes. For instance, they can perform tax fraud, open credit accounts, and make other significant identity breaches. In addition, financial data can be utilized for fraudulent activities and purchases, especially if it lacks robust digital security systems.

#2. Hackers Who Want to Get Into the Digital Infrastructure. Storage and data servers are expensive – and hackers know that.

In order for them to cut costs, hackers may aim to store their applications and data on your infrastructure instead. The better your infrastructure, the more likely cybercriminals are to target it. This can strain your network



to the limits and have devastating effects on your business.

Unsurprisingly, tech companies are some of the most common victims of this type of hacking.

The common indicators that a hacker has tapped into your digital infrastructure include:

- Running out of storage faster than usual
- Your network suffers slowdowns
- You may have unknown devices on your network.

#3. Hackers Who Are After Confidential Information. Few business aspects are as important as your intellectual property (IP). Your products and services enable you to stand out from the competition and strike a chord with the target audience.

A huge problem arises if hackers steal the design of your upcoming product before you launch it or submit your patent. A competitor may obtain the information, allowing them to hit the market first and undercut your sales.

#4. Hackers Who Want to Get Account Data. Sure, you and your IT service provider might have done enough so that hackers might not be able to obtain financial data. But are your employees' accounts secure?

If hackers compromise them, they may let them run scams and gain information to disrupt your operations.

For example, losing CEO login credentials can be devastating. Besides granting hackers access to sensitive information, it also helps them impersonate the CEO. In return, they can solicit information from employees or clients and halt your operations. This data breach can lead to widespread confusion, tarnishing your reputation.

#5. Hackers Who Aim to Have Network Control. In some cases, hackers aren't after data. Instead, they want to gain control of the entire network. And to make it happen, they launch ransomware attacks.

These activities enable them to lock you out of the system and make data inaccessible until you pay a ransom. They're typically initiated through spam, phishing emails, and online ads.

The average ransom amount stands at approximately $30,000, but the loss caused by business disruption is much more significant.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com