TECHMinutes
December 2017
Your Small Business Technology Information Source!

This Issue:

Why Hasn't Mobile Payment Really Taken Off?

Thieves Materialize Most Around the Holidays

Control Where Your Downloads Are Saved

The Value of Outsourced IT

Is Your Organization Utilizing Software from the Cloud?

Two Steps Are Better Than One, Where Security Is Concerned

Control Where Your Downloads Are Saved

Whenever you download a file from the Internet, the file will, by default, go to an aptly-titled folder in Windows called Downloads. Unless you change the default settings, your files will always be saved here. But what if you want to make it so that your downloads go somewhere else? You can accomplish this pretty easily. We'll walk you through how to do it for some of the most popular browsers, including Google Chrome, Microsoft Edge, and Mozilla Firefox...

Read the Rest Online!
http://dti.io/control

About Directive

We are a technology consulting firm specializing in technology implementation and management for businesses. We're known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses.

Visit us online at:
newsletter.directive.com

Why Hasn't Mobile Payment Really Taken Off?

Digital payment options have become commonplace in today's society. In fact, ever since people could purchase goods and services off of the Internet, some of the world's most successful companies are a result of digital payment. It was a natural progression then, as the mobile device boom came, that mobile payment would take the place of cash and/or cards and bring these digital payment options beyond the Internet, and into our retail stores. This simply hasn't happened and here are four reasons why.

The Tried and True Payment Still Works

The first reason is simple. Retailers still accept cash and credit cards. Why would anyone who has been using these tried and true methods of payment for 20-plus years change things up? According to First Annapolis Consulting's "Study of Mobile Banking & Payments", while 64 percent of all smartphone users have used some form of mobile payment platform, only five percent consider themselves frequent payment users. The fact is that it's not as attractive as you may think, and is further relegated to the background because...

(Continued on page 2)

Thieves Materialize Most Around the Holidays

In terms of identity theft, data loss and good ol' fashioned pickpocketing, the holiday season is one of the riskiest times to travel. When it comes to protecting your personal information, thieves and cybercriminals are counting on you to be distracted and make careless mistakes. In 2016, the number of fraud attempts went up by 31% during the holiday season. In addition, credit cards, mobile devices, and open Wi-Fi are common targets throughout the holidays.

Here are a few tips that can help keep you and your family safe from hackers and thieves.

- **Hide the Goods -** Pickpocketing is an old-world method of theft that is still extremely effective - especially in a hectic environment like an airport during the month of December. A favorite target of pickpockets are smartphones. Travelers should avoid storing any personal belongings, including smartphones, in places that are easily accessible.
- **Bring Only Necessities -** Between work and personal uses, most adults have at least three mobile devices. In general, bringing all of them with you while traveling isn't necessary. The more devices along for the trip, the more targets there are for criminals.

(Continued on page 3)

The Value of Outsourced IT

IT maintenance is something of a sensitive topic for some organizations. While most understand that it needs to be done, they often don't have the resources to make it happen, either due to a limited budget or timeframe. How does your business handle IT maintenance? If your organization is having troubles managing its annual technology budget, or if you are consistently experiencing profit-sapping downtime, consider managed IT services the answer to your problems.

Simply put, the traditional method of technology maintenance doesn't work well anymore. The break-fix method to technology management is generally how small businesses have run their organizations for quite some time. Break-fix relies on your business reaching out to a maintenance provider only when your systems are malfunctioning, causing downtime and inefficiency that is sure to show up on your organization's bottom line.

Without a reliable way to guarantee that the downtime-causing issue won't happen again, the break-fix method is like slapping a Band-Aid on a wound and hoping that it won't reopen. Managed IT, on the other hand, is designed to address problems before they happen by taking preventative measures.

Managed IT accomplishes this goal by providing you with comprehensive access to technicians who you can proactively monitor and fix any technology problem you may have with your network or infrastructure. For businesses that lack an internal IT department, managed IT can fill the void you have in technology administration quite nicely. Furthermore, managed IT can provide value even for organizations that have dedicated internal IT staff.

More often than not, a small business will have, at most, an internal team consisting of only a handful of technicians who, more than likely, have a lot on their plate. By supplementing their skills with a managed IT service provider, you're giving them more time to focus on the quality of their work…

Read the Rest Online!
http://dti.io/outsourced

Why Hasn't Mobile Payment Really Taken Off?

(Continued from page 1)

There is a Lack of Incentive

What added value does a mobile payment service actually offer? Sure, in some states that have gone to a digital ID system, this would seemingly allow consumers to forgo the wallet completely. That's it. Most mobile payment interfaces make it difficult for users to redeem loyalty points or take advantage of special offers at mobile point of sale machines.

There are companies, such as Starbucks, that have made a point to integrate their loyalty points system into their mobile payment platform. Their mobile app combines the loyalty point program with mobile payment options, which is great for consumers. But like the consumers themselves, if a company doesn't see an immediate (or even long-term) demand, they will avoid laying out the capital until that demand is present.

In order for mobile users to take full advantage of the mobile payment platforms, you will need to give them some form of incentive to use it. This is mainly since...

Mobile Payment Actually Takes More Effort

One of the claims that mobile payment providers make is that it is much easier to use than any other type of payment. Just tap and go. While this seems reasonable on the surface, the reality of it is that it takes just as long or longer to access your mobile payment platform through your smartphone as it does to take cash or a card out of a wallet. Consider for a minute the steps you have to take in order to make mobile payment work: You have to take your phone out, unlock it, access the mobile wallet app, select which card you want to use, and then hold your phone to the terminal. After this they still need to either sign the screen/paper or provide a pin. Why take so much effort to make purchases when it takes less time to buy goods in a traditional way; and, still have to deal with…

Mobile Payment Security Concerns

To be fair, mobile payments may be as secure as any other form of digital payment, but there is an inherent fear in many consumers' minds that because there is an all-digital transmission of financial information that it is somehow less secure than traditional digital payment options. This fear isn't unfounded, as each day people can read about data breaches at banks, stores, and major online retailers, that only work to fuel the anxiety surrounding mobile payments.

Many cyber security experts have cautiously endorsed the use of secure payment apps, while others point to studies like the 2015 Mobile Payment Security Study that overwhelmingly urges a wait-and-see approach, but does admit that the industry is making headway in the security of mobile financial transactions with the inclusion of account tokenization, device-specific cryptograms, and multi-factor authentication.

In the future, mobile devices will become the only computer we'll need, but will they become the only wallet we'll need? Only time will tell.

Share this Article!
http://dti.io/mobilepay

Thieves Materialize Most Around the Holidays

(Continued from page 1)

Travelers are encouraged to bring only the technology they need.

- **Free Wi-Fi is Not Free -** To conserve mobile data usage, many people are tempted to hop onto Wi-Fi whenever possible without fully comprehending the risks. Some open Wi-Fi access points are easily hacked and you'll likely have no idea what kind of security the connection will have. It might be a bit costly but using your data instead of open Wi-Fi may save you from having to deal with identity theft in the future.
- **Patch It -** It's always a good idea to keep your technology up-to-date with security patches and bug fixes. Many of the large ransomware attacks that made headlines earlier this year could have been avoided by security patches. When traveling, reduce vulnerabilities by patching and updating your software before you leave for your trip.
- **Go Phishing -** During the holiday, phishing scam emails emulate holiday-centric messages. Scams will often appear to be from legitimate establishments like FedEx or Amazon. They will often ask for account or password information - or offer exclusive coupons that need to be downloaded to use. Remember: if it sounds too good to be true, it probably is. Avoid downloading any attachments and never give out your password or account information.
- **Skimming a Bit Off the Top -** For those of you who aren't familiar with card skimmers, the premise behind this type of theft is to copy your credit or debit card information by disguising a scanning device on a legitimate source, like a gas pump or ATM. The scammers are then free to use or sell that information. Skimmers are easily overlooked and protecting your information requires constant vigilance. Whenever you're using a credit card during your holiday travels, look closely at any device that you are going to be swiping your cards on.
- **Social Media for Burglars -** For many, social media is about sharing their good times and memories with friends and family. For thieves, it's a road map to determine when a home is going to be vacant because their owners are traveling and how long they're going to be gone for. To eliminate a breaking and entering from your holiday season, avoid posting specifics of your trip information on social media.

Approximately 100 million Americans are going to be traveling this holiday season - meaning that there is no shortage of potential victims. By following these tips, you are taking a proactive approach to keeping your identity and finances safe.

Share this Article!
http://dti.io/thieves

Is Your Organization Utilizing Software from the Cloud?

All businesses require at least some type of software in order to perform as expected. It's how organizations acquire this software that has a considerable impact on cost. For some, software can be a budget-breaking nightmare, but others have found a much more convenient way of acquiring this software: as a service.

Software as a Service is a method of software distribution designed to help your business acquire the applications it needs without suffering from the large upfront costs that software acquisition typically carries with it.

Do you remember purchasing software licenses for each and every user on your network? This can get somewhat challenging to maintain, as these licenses need to be renewed frequently, and if they are not, your organization could be put at substantial risk.

Businesses can instead use software as a service offerings to purchase access to cloud-based applications and storage. Basically, you pay for access to the software and reap all of the benefits of actually owning it--plus some additional ones--by leveraging cloud computing.

More Cost-Effective

Think about how much it costs to purchase software for your organization. The same services that are necessary for operations, could be a major detriment to turning a profit. With the use of an application hosted in the cloud, you can cut the cost of ownership and transfer the once recurring capital expense into a manageable operating expense.

Up-to-Date Editions

When you purchase software as a service applications, you always access the most recent version of it through an online interface. This means that you'll never have to worry about updating the apps with patches or security updates, as they will be taken care of by the service provider.

More Flexibility

Purchasing new software licenses can be troublesome, especially when you're a small business that's experiencing growing pains. You can add new users easily enough just by creating accounts for them--no additional purchases necessary. Changes in your service plan are generally added on your next billing cycle. This provides the scalability every growing business needs. Does your business want to use software as a service?

Share this Article!
http://dti.io/softcloud

We partner with many types of businesses in the area, and strive to eliminate IT issues before they cause expensive downtime, so you can continue to drive your business forward. Our dedicated staff loves seeing our clients succeed. Your success is our success, and as you grow, we grow.

Two Steps Are Better Than One, Where Security Is Concerned

You're lucky to go a month without seeing news of some devastating data breach. With more businesses gearing up for the worst, what are you doing to protect your organization's intellectual property and sensitive data? You can start by implementing a new type of authentication system that's much more secure than your current security strategy--two-factor authentication.

It's no secret that a password is no longer as secure as it used to be. Advanced technology used by hackers can crack even the most secure passwords with enough time. This is because many users tend to opt for passwords that are either easy to guess, not complex enough, or are simply quite obvious for one reason or another. We'll walk you through some of the common scenarios that you might encounter for password security, and how two-factor authentication can solve it.

For example, many users have to change their passwords so frequently that they may be mind-boggled about how to remember each and every one of them. Proper passwords should be at least 12 characters long, including special characters, both upper and lower-case letters, numbers, and symbols. The best way to approach building a password is to include all of this information in a seemingly random string, but users will often try to use something that they will remember--information that can often be stolen during a hacking attack, or found on social media.

What if you use your first-born's name in your password? That's information that could easily be found in public records. The same can be said for the name of your parents, which school you went to, and even your favorite TV show via social media. Thanks to the Internet, hackers have all of the tools they need to find plenty of information about you--information that you might subconsciously be using either as a security question or for a password.

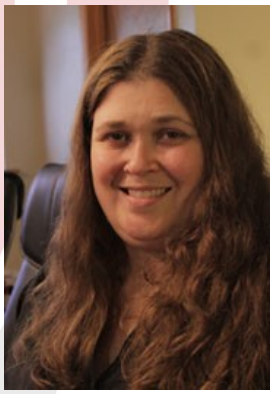
Therefore, if you are taking advantage of a complex password, it makes sense from a logical standpoint that you would only want to remember one of those, at most, at any given time. Unfortunately, this has a negative side-effect on security, because if a hacker gains access to one account through the password, they will have access to all of your accounts through the password.

Password managers make it easier to remember complex passwords, but the issue remains the same. If a hacker has access to your password, what keeps them from accessing your accounts? Two-factor authentication is the answer. Two-factor authentication essentially adds a secondary level of security to any online account or network access point. Where you once may have needed only a password, you'll now have to use some sort of secondary credential, be it a mobile device or an email to a secondary account. It's just one small way you can protect your organization, and it doesn't take long to set up.

To learn more, reach out to us at 607.433.2200.

Share this Article!
http://dti.io/twostep

Chris Chase
Solutions Integrator



Charlotte Chase
Solutions Integrator

Directive

330 Pony Farm Road
Suite #3
Oneonta, NY 13820
Toll-Free 888-546-4384
Voice: 607-433-2200

Visit us **online** at:
newsletter.directive.com

newsletter@directive.com
facebook.directive.com
linkedin.directive.com
twitter.directive.com
blog.directive.com
instagram.directive.com