ISSUE
01
January 2020

MANAGEDTEK
MONTHLY
JOURNAL OF
INFORMATION

TekTimes

This issue

Welcome!

Happy New Year and welcome to our first monthly newsletter of 2020! ManagedTek's monthly newsletter is to keep our customers updated about our services and what's going on in this vast world of technology.

MANAGEDTEK: ON THE FRONTLINE

The advisor role is a powerful one: Managed Service Providers (MSP) support all parts of the organization while increasing use of cloud and other services by the customer makes the problems of security less directly manageable. The MSP can provide solutions to enhance security awareness across the organization and make all employees more aware. MSPs are becoming pro-active – with monitoring and helping with risk-assessment. The MSP can provide industry and sector-specific guidance, not only just from a regulatory or a fine perspective, but looking at the impact on reputation and with a response based on infrastructure strengthening.

Year In Review – 4 Phishing Attack Trends of 2019

Few cyber threats are as prevalent and costly as phishing attacks. In 2018, Microsoft documented a 250% increase in phishing campaigns, which masquerade as legitimate products or services but carry malicious payloads that steal credentials and compromise IT integrity.

To no surprise, the rise of phishing attacks continues to trend upward and is wreaking havoc for SMBs and enterprises alike. Even as companies implement automated defenses intended to keep phishing attacks out of employee inboxes, many inevitably make their way through. A recent survey found that nearly half of respondents reported malicious emails reaching employee inboxes every week, and 20% indicated that they experienced a data breach because of a phishing vulnerability.

To maintain an edge, hackers are continuously evolving their strategies and improving their attack methods, making their efforts increasingly difficult to detect. In other words, employees may not be fooled by phony emails from a foreign leader or celebrity, but they could be compromised by a call or IM from their manager or CEO. Continuing you will find outlines of four of the latest phishing attack trends that you'll want to know in order to protect your business.

#1 Increased Personalization

The past several years have seen billions of records compromised, and the consequences far exceed the immediate media scrutiny and consumer backlash that follows in the wake of breach. Cybercriminals are repurposing exposed information to craft sophisticated phishing campaigns that are camouflaged with authentic-looking information purportedly from known and trusted sources.

#2 Multi-platform Approaches

Phishing scams are commonly associated with email messages, but today's cybercriminals are taking advantage of diverse communication platforms to posit messages in our various inboxes.

#3 HTTPS Encryption

In addition to reaching users in familiar territory, hackers are deploying the internet's sign posts of security to elicit the trust of their victims. Specifically, cybercriminals are manipulating HTTPS, the internet protocol that denotes encryption and security, to trick users into a false sense of security.

#4 Dynamic BEC Campaigns

Between the treasure trove of data available on the Dark Web to the information readily published on company websites, hackers can effectively impersonate higher-ups or IT administrators with staggering effectiveness. Business Email Compromise (BEC) scams rely on personalization, and today's hackers dialogue directly with their victims to gain trust.

YOUR BUSINESS CREDENTIALS: A HACKER'S HOLE-IN-HOLE

Digital credentials, such as usernames and passwords, connect you and your employees to critical business applications and online services. Unfortunately, criminals know this — and that's why **digital credentials are among the most valuable assets found on the Dark Web**.

CYBERSECURITY GUIDELINES:

HHS has issued cybersecurity guidelines in an effort to drive voluntary adoption of best practices. Such guidance could signal impending legislation to continue to progress as technology continues to evolve, so ManagedTek's experts curated some key takeaway.

LEARN HOW TO IDENTIFY PHISHING:

With the number of spam emails sent daily expected to increase to almost 190 billion a day through 2023, it's increasingly important to be able to spot the tell-tale signs of a fraudulent email and protect your personal and business data, and your tech from malicious viruses and malware.

Your Employees: Your First Line Of Defence:

Whether it's born out of innocent curiosity or malicious intention, email being the main form of business communication poses different threats to organizations and individuals. Spam mail and phishing attacks can often be detrimental to an organization, these attacks can cause a breach of personal or clientele information, or a loss of funds. The best way to avoid and protect yourself from an attack is awareness and education. Knowing the different types of attacks, motives and identifying key features can help yourself and employees avoid malicious emails. Having a program specifically designed to simulate phishing attacks and provide in depth security campaigns will reduce your risk of falling victim to a scam through employee education. From monitoring your organization's domain for compromised credentials to deploying identity and credit management programs to protect the employees and customers you serve, ManagedTek has the solution.

It's evident that phishing scams will continue to keep IT admins up at night for years to come.

This is the easiest thing to lose: email addresses, passwords, credit card details… with just small elements of this data, criminals can deduce passwords, create hacking strategies and gain access to sensitive information, which they can then sell to the highest bidder.

However, there is a silver lining. Unlike other cyber-attacks, phishing scams are only effective if they are acted upon, and companies can mitigate such threats with regular, comprehensive awareness training to their employees.

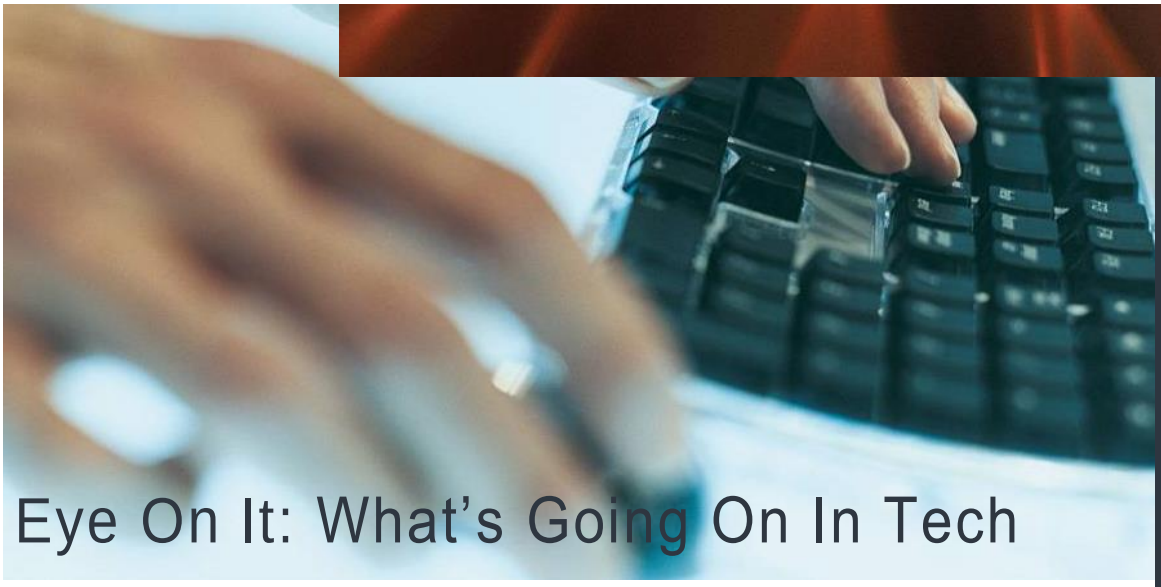
With the right solutions provider, you can equip your employees to stay abreast of emerging threats, report potential misuses of data, and transform themselves into the first and best line of security against cybercriminals. Whether you're a small business or large enterprise, you have the power to stop phishing attacks from stealing employee credentials or proprietary information.

While you can't mitigate risk entirely, you can be more in control. Dark Web ID can detect and monitor what information from your company is being trafficked on the uncharted web.

Trained and aware employees are critical to securing an organization, and an effective, ongoing internal security awareness program can help reduce your company's vulnerability, turning the "weakest link" in your cyber defenses into its greatest strength.

As public vigilance of security and privacy continues to increase, being featured in headlines as the victim of an insider attack poses serious consequences for brand equity and customer loyalty.

To add value to our customers, ManagedTek, provides solutions that include Security Awareness Training and Anti-Phishing platforms.



Eye On It: What's Going On In Tech

Of course you heard....January 14, 2020, Microsoft will end support for Windows 7 and Office 2010 October 2020. Of course you can still utilize, but Microsoft will not update, fix or support software, security or technical issues after these dates. If a new threat emerges, hackers can — and likely will— take advantage, posing a serious cyber security threat to your business. Are you prepared?

Microsoft will continue to provide updates for the Microsoft Security Essentials (MSE) app, which is the built-in antivirus program included in Windows 7.

Department of Homeland Security (DHS) updates its view of trust in new network security guidance Reducing risk one decision at a time. These "trust zones" updates are aimed at "shifting the emphasis from a strictly physical network perimeter to the boundaries of each zone within an agency environment to ensure baseline security protections across dispersed network environments."

Contemplating where to start? Too often people worry about a hacker stealing their data, breaching their security, and taking off with their money.

Stop the worry, learn more about affordable workstation security with IT support. Security has evolved from downloading free software. Today, we need someone watching and reporting.

We support you by managing and monitoring your systems and networks. Our goal is to make it easy for you to focus your energy and passions on your business while we take care of your technology needs. Technology made simple by creating a solution to meet your specific need.

This Month's Q&A TeK Tip

Q: What is the "Dark Web?"

A: The Dark Web is made up of digital communities that sit on top of the Internet, and while there are legitimate purposes to the Dark Web, it is estimated that **over 50% of all sites on the Dark Web are used for criminal activities**, including the disclosure and sale of business credentials. Far too often, companies that have had their credentials compromised and sold on the Dark Web don't know it until they have been informed by law enforcement — **but by then, it's too late**.

At ManagedTek, we specialize in protecting businesses just like yours from falling victim to increasingly complex threats. **We offer Dark Web Monitoring** to identify exposed credentials and alert our customers before hackers can do harm. We also offer our **Security Awareness Training** platform in order to train your employees to recognize and avoid phishing attacks and other malicious activities targeting human vulnerability.

Cyber Awareness Strategies:

Cyber awareness trainings. Users are the weak link in security. Are you training your team to recognize cyber threats?

Keep Updates Up to Date. Does your organization have any missing security updates?

Reduce Supply Chain Vulnerabilities. Don't let security incidents from your supply chain become headaches for your organization.

Upcoming Events:

New Office Location Grand Opening – TBT

ConnectIT Global – May 4-7, 2020.

ManagedTEK
ManagedTek
1090 Adams St.
Suite G
Benicia, CA 94510
www.managedtek.com | 707.205.3727