Dimensional Dispatch

7th Dimension Newsletter

7th Dimension
5005 Windplay Drive, Ste. 1
El Dorado Hills, CA 95762
(916) 221-0855

September 2018

"INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY"

Why Your Website Is Officially 'Not Secure'

In 2017, Google's Chrome browser started marking transactional sites that weren't using HTTPS as "not secure".

On 24 July – think of it as the Google **Chrompocalypse** – that "transactional" vs. "everything else" difference comes to a decisive end. Now, all HTTP pages will be slapped with the "not secure" label, regardless of whether they're transactional or not.

For more than a decade, the browser address bar has been the place where we all (**hopefully**!) looked to see whether the site we were visiting had the reassuring "Secure" padlock, letting us know that the pages we were about to view were coming to us over a secure connection. That padlock let us know that nobody else on the web could intercept the information we exchanged with a given site, and updates within our own IT infrastructure in line with best security practices. In its ongoing efforts to make **encrypted** – i.e., HTTPS – web connections the norm, as opposed to the exception, we can all welcome Chrome version 68.

With **Chrome 68**, Google takes one more step toward streamlining that address bar, moving to the point where it only informs users when a site is insecure. It gets better from here: Starting with **Chrome version 69**, due 4 Sept., the "Secure" label will disappear from HTTPS sites, and the green padlock will turn grey.

At some point after that, the padlock will go "Poof!" completely disappearing from the address bar, leaving it empty save for the URL. No more telling us when something is **good (HTTPS)**. We'll just be told when it's **bad (HTTP)**.

We still have to be careful. But we're waving a hearty hello to Chrome 68 just the same: it's one important stepping stone on the road to a more secure web. (Sophos)

IN THIS ISSUE

What Will You Do When This Disaster Hits Your Business?

Every savvy business owner knows the necessity of locking down data—however, many cybersecurity technologies are woefully out of date. Sure, your current solution may have worked great, but digital threats to your company constantly evolve. Criminals will eventually attempt to breach your data — and your barriers are not as secure as you might think.

Before World War II, the Germans developed its family of infamous Enigma machines. These devices, about the size of a small microwave, were composed primarily of a typewriter and a series of three or four rotors. By using a set of rules contained in a corresponding codebook, German soldiers used the machine to encode vital messages to send covertly over the airwaves. The number of potential permutations — and thus solutions — for the code was in the tens of millions. The Germans were confident that the code could never be broken and used it for top-secret communications.

The code's impenetrability didn't last. Via photographs of stolen Enigma operating manuals, the Polish Cipher Bureau reconstructed one of the stubborn Enigma machines, internal wiring and all, enabling them to decrypt the Wehrmacht's messages from 1933 to 1938. Facing an impending German invasion, Poland decided to share these secrets with the British. But, at the outbreak of the war, the Germans increased the security of the Enigma initiative by changing the cipher system daily. In response, a British code-breaking team, led by genius

English computer scientist Alan Turing, constructed primitive computers, known as "bombes," that allowed them to decrypt the incredibly complicated ciphers faster than ever before. But

it wasn't until the capture of the U-110 warship and the seizure of its Enigma machine and codebooks that the British were able to decrypt the most complicated cipher of the war, the Kriegsmarine Enigma. The information gleaned from these decrypts are believed to have shortened the war by more than two years, saving over 14 million lives.

Just like you, the Germans believed the systems they had put in place to defend their secrets were impenetrable. However, there were flaws in German procedure, mistakes made by Enigma operators, and failures to introduce changes into the Enigma formula — along with the Allied capture of key equipment and intelligence — that allowed the Allies to crack the code once and for all.

Take this as a cautionary tale: the most advanced, complex cryptography system in the world became obsolete within 10 years. The same goes for your potentially outdated cyber security measures.

Though they may not be led by Alan Turing, criminals are constantly chipping away at the defenses of even the most powerful firewalls. The arms race between cyber security companies and cybercriminals rages on behind the scenes, and you can bet that they've already cracked your business's "Enigma." Just look at the massive European cyber-attack this past June, which infected computers from over 27 companies across the continent, including those of the largest oil company in Russia, with ransomware. The unimaginable cost of that attack is something you certainly don't want your business to shoulder.

As technology evolves, so does crime. New threats arise each and every day. While solutions are available (and needed), they are notably absent in older software developed at a time before these constantly morphing attacks even existed. Luckily, you have your trusty IT provider, constantly on the lookout for cutting-edge solutions that protect our clients from even the nastiest malware.

Don't be like the Germans. Constantly look at options to upgrade to more robust, better cyber security to defend yourself from the bleeding-edge hackers, and sleep safe knowing your business is secure.

HAVE YOU REVIEWED YOUR IT SECURITY LATELY?

Call us at (916) 221-0855 to schedule an up-to-date network scan.

3 Devices That Could Be Spying On You

With the rise of the internet of things, there's potentially a computer chip, camera, microphone, or sensor in many previously "dumb" devices around your home and office. As a result, privacy concerns have grown.

1. Smart dolls and teddy bears - Walk into any kids room and you're likely to find stuffed animals or dolls.

The latest generation of talking companions could be collecting information on kids and transmitting that data back to the toy manufacturers' servers, which may or may not be secure. And in the case of aptly named CloudPets, voice recordings of over 1 million customers were stored in the open on public-facing servers, accessible to anyone.

2. Internet-connected cameras - Many IP cameras utilize default passwords, making them trivial to hack. And this fact is alarming, considering these devices record audio and video of people's lives, often giving a glimpse into private spaces and conversations.

Making matters worse, unsecured security cameras are often available on the open internet for everyone to see. Additionally, some camera manufacturers' firmware might have critical vulnerabilities that make them easy to hack.

3. Cars and drones - These days, cars are basically highly-advanced computers on wheels. Many are equipped with microphones, GPS, Bluetooth, wireless entry systems, self-driving features, and internet connectivity. But convenience can come at a cost.

Recent allegations from Wikileaks claim government agencies are able to hack into car systems, making both eavesdropping and potentially taking control of the vehicle itself possible. If all of this sounds like far-fetched science fiction, know that in 2015, 1.4M cars were recalled due to a vulnerability in Chrysler vehicles that among other things, allowed hackers to engage the brakes of the car remotely.

In these early days of connected devices, it should come as no surprise to you that these vulnerabilities will continue to be discovered. While smart devices surely can be beneficial and even revolutionary, it's also important to weigh the benefits vs the potential vulnerabilities they can introduce. (Spiceworks)

7TH DIMENSION

IT without limits

5005 Windplay Drive, Suite 1, El Dorado Hills, CA 95762
(916) 221-0855
support@7thdi.com

We love having you as a customer, and quite honestly, we wish we had more like you!

Simply refer any company and earn up to $100 when your referral becomes our client.