March 2016

# SecurityAwarenessNews

the security awareness newsletter for security aware people

## Personal & Home Network Security

# SECURITY@HOME

CONFIDENTIAL

Following policies and protocols at work is not always easy. The IT department will configure office devices according to business needs. The most important things you need to do are follow policies, use common sense and, when in doubt, ask. A healthy dose of skepticism is essential for all of our collective security well-being.

But at home, ***you*** are the boss and the IT department. It is your responsibility to ensure your home network is secured in all three domains - cyber, physical and human. And, as usual, most of it comes down to common sense!

We live in a world where seemingly every device has the ability to connect to a network. From media players and fridges, to gaming consoles and smart TVs, our homes have become an Internet of Things. ***Every one of these connected devices poses potential security risks.*** It's more important than ever to implement strong home security 'best practices,' similar to what you are expected to follow here at work.

For example, if you've purchased a TV in the last few years, chances are it's a *Smart TV*, which gives you access to thousands of apps and the ability to connect to your home network and browse the Web. For all intents and purposes, your TV is a computer. As such, it is plagued with many of the same vulnerabilities as your laptop and needs to be protected accordingly. In 2013, during a presentation at Black Hat, two researchers proved the vulnerability of the then-early models of smart TVs by hacking the host operating system, which provided them access to things like the webcam and account credentials for various social media sites. ***Everything—including browser history, cookies and network credentials—was accessible.*** Samsung made the news when it said it collected voice commands and possible 'room conversation' (as well as, potentially, video) from smart TVs. **Click here to read more.**

Device manufacturers have since upgraded the security lapses of their first generation products. But vulnerabilities will always exist. We must pay attention and employ our security awareness skills, not just at the office in our professional life, but in our mobile and personal lives as well.

**THEY CAN HACK MY CAR!?**

**http://blog.thesecurityawarenesscompany.com/important-security-vulnerabilities-in-modern-smart-cars/**

## Where to Begin?

**With proper security guidelines in place, we can protect our data and still enjoy all of the convenient wonders of technology. Consider the following tips as a starting point for using all those smart devices.**

1. Turn off all unneeded network connections until required for a particular task. Remember to turn them off when done!
2. **If you are connecting to the internet with your TV or gaming console, install an antivirus app and turn on the firewall if one exists.**
3. Only install apps from verified sources. Spend time researching an app, reading reviews before installing.
4. **Know what devices are connected to your home network(s) as well as to mobile phones, VoIP and physical security systems. One breach and it's Game Over.**
5. Turn on auto-update so your device is always on the latest version of software. Most often, software updates provide patches for security holes.

Good security comes from timely response. Report security incidents immediately!

# Protecting Your Home Network

Whether you live in a secluded neighborhood or an active apartment complex, protecting your home WiFi network is just as important as keeping your front door locked. The out-of-the box configurations for wireless routers include easy-to-hack settings that need to be changed immediately. **We can better protect ourselves by following a few basic procedures that require minimal computer skills.** Here is a great step-by-step list provided by the FCC as a guideline to personal network security: fcc.us/1U3VxtB.

There are a few advanced, more technical options that will provide an extra layer of security. You could install a VPN (Virtual Private Network) client on your mobile devices. You could consider not broadcasting (hiding) your WiFI network name (SSID). You should consider using a password manager to keep track of and update your passwords!

# A Security Policy for the Whole Family

Have you ever thought about creating a family security policy? Enforcing a simple policy will help keep everyone responsible and worry-free; have everyone sign!

Below are some suggestions that you could add to your family's security policy.

**Keep your devices up to date.** Routinely check for software and firmware upgrades so you're always on the latest (and thus most secure) version.

**Trust but verify.** Never give out the password to your WiFi network to anyone except trusted friends and family. For occasional visitors, you should set up a guest network that is separate from your personal network.

Most gaming consoles and media devices can download and install apps, movies, and games. **Never download anything that doesn't come from a verified source.** It's also a good idea to use a prepaid debit or game network card to make purchases rather than using a credit card. Should a breach occur, you won't have to worry about your credit card data getting leaked.

**Create different accounts on shared devices.** Your kids shouldn't have access to the Admin account. Create yourself a 'User' account for non-Admin functions. Under your Admin account, you can block websites per user, monitor activity, and make sure the quick-clicking kiddos don't delete important system files!

**Have a master backup, and backup to it regularly.** Nothing is worse than losing years of photographs or family videos thanks to a hardware failure. Designate a pair of drives to backup your data for redundancy and use an automated backup program every day. Use a cloud backup service for added redundancy and accessibility. Experts suggest a primary 'local' backup and the Cloud as a third. In case your local back up and main machine are both affected by a disaster, you can still recover your data.

**This printable Human Firewall Pledge can be used for security policy inspiration: bit.ly/1S8t4lw**

# Hey! That's my pie! Oops, I mean my P-I-I!

**Remember our credo: don't share pie.** Or, more accurately, don't share PII (personally identifiable information). What qualifies as PII? PII is any information that can be used to identify an individual. Full names, email addresses, and national identification numbers are just a few examples. Naturally, if it's sensitive information—read, information useful to criminals—it will be sought after information, and needs to be protected.

**Never underestimate the power of the word *"why"*.** When filling out a form of any a nature, ask: *"Why do you need my Social Security Number?"* and *"Why do you need my date of birth?"* and, perhaps more importantly, *"How are you protecting it?"* Qdoba doesn't need your mother's maiden name when you sign up for their rewards card. Remember: security starts with **you** and the information you give out.

**The internet is forever.** Anything you or your family puts out there will be there forever, even if you delete it. Don't tell the entire internet that you'll be gone to Peru for two weeks, leaving your house empty and ripe for robbery. Teach your kids that tweeting a photo of their newly acquired driver's license is a terrible idea. When taking selfies, study the photograph to ensure that no personal information accidently ends up the background. Once it's out there, it's out there for eternity.

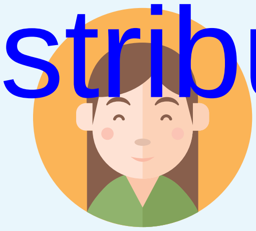
**Teach your kids.** Your children won't be tech savvy unless they are taught to be. Communicating as a family about privacy risks will ultimately improve your family's security posture. So, when you approve them joining the next hip social network, get involved in their profile setup so you can guide and monitor the security and privacy settings. It can help if they include you as a *'friend,'* too.

**Setup junk email accounts.** When signing up for social networks, websites, forums, coupon sites, and the like, don't use the same email account you use for personal or business communications and file sharing. This will help keep the scammers locked out of your personal and professional networks.

## What the Experts Do:

**W • 63 • CEO**

*"I refuse to give out unnecessary information. Ask my wife; she's heard me argue with everyone. Also, separate email accounts! I have a collection of emails that aren't linked to my real identity that I use to sign up for non critical stuff."*



**J • 45 • InfoSec Awareness Program Manager**

*"I monitor all of my kids' social media activity and limit which networks they can use. No Snapchat for them since I can't track it but Twitter, Instagram and Facebook are all okay."*

**D • 35 • Security Engineer at HP**

*"I monitor all of our financial accounts and credit reports weekly, looking for anything out of the ordinary. I also swear by my password manager which securely syncs all of my personal devices."*

Good security comes from timely response. Report security incidents immediately!

# RANSOMWARE

## What is it?

Ransomware is exactly what it sounds like: ***malware that holds you, your computer and your data hostage for a ransom.*** It works like this: You open an email with an attachment. You choose to download and open the attachment. The attachment contains malware that assumes control of your computer and, most often, encrypts your data so you have no access to it. In turn, if you pay the ransom, which can be anywhere from $300 to $17,000, the hackers promise to unlock your computer.

In short, it's a phishing scam bundled as scareware with a financial return for the bad guys. One of the primary targets has been Wordpress, and now Joomla is in the crosshairs.

### I Got Ransomed... Now What?

Bad things can still happen to the most security aware of us. So what do you do if your computer is held for ransom? Do you pay the hackers the money and hope to get your data back? Only you can place value on your data, and determine if the asking price is worth the recovery. **There's no guarantee the hackers will unlock your system even if you do pay.** In general, it's best not to negotiate with terrorists. Instead, keep your data backed up for easy recovery, and (as always!) think before you click. (Please remember, at work, always follow policy. When in doubt, ask for help!)

## How to Avoid It

Protecting yourself, your family and your business from ransomware requires you to follow four easy steps that we're all familiar with and, since you're security aware, you're probably already doing!

1. **Stay up to date.** As always, there are reasons why software companies are constantly rolling out updates, and they're usually security related. This is especially true of websites. If you run a CMS (content management system), a blog or other website, keep it (including plugins and themes) updated with the latest patches.

2. **If the email seems phishy, it is.** Always, always, always verify the source of an email before downloading or clicking on any attachments. Even simple things, like a flight confirmation with an attached itinerary, have been known to be phishing scams. Think before you click. When in doubt, delete.

3. **Backup your data every day.** Hostages are only as valuable as their relative worth. If a criminal hacker holds your computer at ransom, but you have all of the pertinent data backed up elsewhere, who's in charge? Both external hard drives and cloud storage are inexpensive compared to the cost of ransom.

4. **Know how to recognize antivirus popups and warnings.** Rogue security is no different than ransomware. You'll see dialog boxes that pop up on various websites claiming to make your computer faster or insisting that you have a virus. Clicking these boxes will install rogue security which will make your system vulnerable to ransomware.

Good security comes from timely response. Report security incidents immediately!

# HEADLINE NEWS

## Ray Tomlinson, Inventor of Email, has Died at 74

Ray Tomlinson sent the very first email back in 1971 while looking for any problems that ARPANET – a precursor to the internet we have today in development at the time – could potentially solve. He did so with the SNDMSG command, creating with it the first messaging program that sent files across networks. He was also responsible for designating users from hosts with the @ symbol, an icon that is now etched onto our collective consciousness.

Tomlinson died of a heart attack on March 5th. Needless to say, we modern technophiles have a lot to thank him for, and his integral role in shaping the course of networking means that he will never be forgotten.

Read or listen to an interview from NPR with Ray Tomlinson about his important invention (reposted in memoriam) here: n.pr/1R3f8da.

## How do you know if your smartphone has been compromised?

Has your smartphone been acting weird lately? Are the apps malfunctioning? Do you seem to be making and receiving calls that you don't remember? Is your data usage always way over what you expect it to be? These are all signs of a compromised smartphone.

More and more of us are relying on our smartphones to do everyday tasks like sending emails and paying bills. Smartphones are just as vulnerable as computers and we should always take steps to prevent them from being compromised. We Live Security has an excellent article that you can read here about all the signs of a compromised smartphone and the steps you can take to prevent it from happening in the first place: http://bit.ly/1QvSjxE.

BBC

**BBC News** @BBCNews · Jan 15
Hyatt names hotels hit by payment information malware http://www.bbc.com/news/technology-35322394

R

**Reuters** @reuters · Mar 8
Home Depot agrees to pay $19.5M to compensate for 2014 breach reut.rs/1UQV5hQ

K

**Krebs on Security** @briankrebs · Mar 6
Seagate falls for phishing scam, exposes W-2 docs on all employees bit.ly/1QAPxq5

T

**Threatpost** @threatpost · Mar 4
APT espionage campaign Operation Transparent Tribe targets Indian diplomats & military personnel bit.ly/1TLNz93

INQ

**The INQUIRER** @INQ · Mar 2
New Mac malware tied to infamous Italian "Hacking Team" bit.ly/1Ld22YD

US

**US Attorney EDNY** @EDNYnews · Mar 1
Turkish hacker Findikoglu pleads guilty to $55M cybercrime heist 1.usa.gov/1RkdePJ

DM

**Daily Mail Online** · @MailOnline · Mar 9
Facebook's 'Like' button violates European privacy laws http://dailym.ai/1U3A9EN

NS

**Naked Security** @NakedSecurity · Jan 11
Could your smartwatch be giving away your ATM pin? http://wp.me/p12OrT-1iST

Good security comes from timely response. Report security incidents immediately!