Security Snippets — August 2019

A monthly compendium of cybersecurity news

Security at [organization]

Enter your security news here (or delete this row).

Hot Topics

This newsletter contains links to online news articles and websites. Before clicking, see "Should You Trust the Links" way below.

Phishing emails are getting better at fooling us. They used to be filled with typos and grammatical errors. Some new phishes look like legitimate requests to collaborate on documents from cloud-based, file sharing services, like SharePoint, Office365, or Box. These may contain malicious links or just take you to a fake login page to collect your account credentials.

As always, if you're not expecting an attachment or a link, don't click. Contact the sender using a known-good method (phone). Don't respond to the email asking if it's legitimate – bad guys are using chatbots to automatically reply.

October is National Cybersecurity Awareness Month! In preparation, DHS published a great set of short documents with tips on how to "Own IT, SecureIT, and Protect IT."

Cybercrime / Hacking

Has a hitman been hired to kill you? Or maybe the CIA is investigating you for child porn. There are all different types of extortion emails out there. And old scams continue to defraud us of millions, like check cashing and romance scams. (But Snippets swears it was true love!)

Frank Abagnale, the famous con man turned FBI Academy instructor who inspired the Leonardo DiCaprio character in the movie Catch Me if You Can, says technology makes crime "4,000 times easier."

Home / Personal Issues

40% of kids in grades 4-8 have connected or chatted with a stranger online. Parents, your kids need more oversight online. And the FTC recently posted a short article about talking with your kids about online safety.

A security vendor wrote a very good article on data and device security. It was written for domestic abuse survivors and contains good tips for everybody.

Do you play Fortnite? Be careful – a new ransomware family is specifically targeting you. It masquerades as a Fortnite hack tool. Make sure you have good backups and learn more about ransomware.

Politics / Legislation

The Democratic Party deepfaked its own chairman to highlight 2020 concerns. Gee, Snippets didn't realize deepfake is also a verb.

Privacy / ID Theft

China has a social credit system where they penalize citizens for “unsocial” behavior, like criticizing the government, visiting unauthorized websites, associating with a person who has a low credit score, buying too many video games or junk food, or letting your dog bark too much. That could never happen here in the U.S. Right? Right??

You might want to be aware that more than 9 in 10 pornography websites send user data to at least one third party. Hey – Snippets doesn’t judge!

Here’s how to delete Siri, Alexa, and Google recordings.

“We anonymize your data before sharing it.” So, you don’t have to worry about being identified. Right? Right??

Best Practices / Risk Mgmt

Billions of website passwords have been hacked. Google has a Password Checkup add-on for its Chrome web browser that displays a warning whenever you sign in to a website using "one of over 4 billion usernames and passwords" that have been hacked. Or you can just search a database of hacked passwords.

And here’s a good list that explains seven ways hackers steal your passwords.

There’s an app called Bluetana that helps detect credit card skimmers at gas pumps by analyzing Bluetooth wireless signals. (Many skimmers use Bluetooth to transmit their stolen data.) Arizona Weights & Measures has a great skimmers site. Scroll down to see how many have been found so far.

Quotes of the Month

To be trusted is a greater compliment than being loved.
— George MacDonald

We may have all come on different ships, but we’re in the same boat now.
— Dr. Martin Luther King Jr.

All the world is made of faith, and trust, and pixie dust.
— J.M. Barrie, Peter Pan

Bonus!

In a world gone mad, sometimes you just need to see pictures of cute baby animals.

Happy 28th birthday to the World Wide Web (on August 6).

Questions & Feedback

Security Snippets is brought to you by the Arizona Counter Terrorism Information Center (ACTIC), the Urban Area Security Initiative (UASI), and your organization. Its purpose is to increase Arizona’s cyber resilience by helping you learn more about security and privacy so you can better protect yourself and your family.

Important: It is up to you to make sure you take the proper steps to secure your home networks and devices. The ACTIC is not responsible for your personal devices.

Contact Snippets at ACTIC Cybersecurity with any questions, to provide feedback, or to be added/removed from this distribution. Please note that this email address is not monitored 24x7.

Any views or opinions presented in this newsletter are solely those of the author and do not necessarily represent those of the ACTIC. Reference to any specific commercial product, process, service, link, or the use of any trade, firm or corporation name is for the information and convenience of the reader, and does not constitute endorsement, recommendation, or disparagement by the ACTIC.

Should You Trust the Links	This email contains links. Should you trust them? Thanks for asking! So, let’s examine this message. It contains the ACTIC’s standard header, states its purpose is to increase your security awareness, and doesn’t threaten or ask you to respond immediately. The verbiage is conversational, rather than formal and attempts to be interesting and entertaining, as well as educational. And you probably signed up to receive this newsletter. Snippets says to trust it, but what do you think? Send an email to ACTICCybersecurity@azdps.gov. (Hint: Hover your mouse over any link to see where it’s really going.)