Consumer, Consumer Threat Notices

A Year in Review: Cybersecurity Highlights of 2015

By Gary Davis on Dec 23, 2015

Like 3 G+1 0 Tweet Email

As 2015 comes to an end, it's time to start scribbling down our New Year's resolutions, and take time to reflect on the past 12 months. It's therefore time to revisit this year in cybersecurity, as we start to look ahead at what 2016 may hold. So put another log on your digital fire, kick back, and take a look at some of this year's best (and worst) in cybersecurity.

Children's toys and services are targeted:

VTech, a purveyor of educational Internet-connected children's toys, did not have a good year. About five million parents and six million children had their account credentials — containing personally identifiable information, photos, and chat logs — compromised. Simply put: it was one of the largest hacks this year.

But VTech wasn't the only children's company to be hacked this year. Japanese company Sanrio, owner of the Hello Kitty brand, had its fan site database leak in late December, according to WIRED. The compromise contained full names, birth dates, email addresses, and more. Some data, like passwords and answers to security questions, were encrypted. Data elsewhere in Sanrio's system lacked stringent security controls, making many of these credentials potentially decipherable. The number of victims alone is staggering, standing at 3.3 million people—many of whom are under 18.

Consumers are blackmailed:

Patrons of Ashley Madison — an online service bringing together consenting adults for affairs — had their emails, credit card data and more stolen from the company's website in late June. The fallout affected 37 million people, and also introduced a rising trend into the realm of cybercrime: hackers blackmailing consumers or companies for profit.

The Ashley Madison hack was one of the first times we saw cybercriminals blackmail both a company and its customers directly. The incident has been a good reminder that what goes online stays online, and has exemplified how far-reaching consequences of attacks like this can be.

Medical records are compromised:

2015 also saw quite a few personal medical records leak on the Internet, such as in the Premera Blue Cross breach in March. It's no mystery why: medical records are unique to you, and cannot be changed, falsified, or easily protected from abuse. This usually gives medical data a long life on the black market. After all, this type of information usually includes full names, birthdates, prescriptions, conditions, operations and more — all things that are very difficult to change or protect.

Card security tightens up:

It wasn't all bad news this year. We also saw the introduction of the Chip and PIN standard in the United States. Chip and PIN technology is a security mechanism making it difficult for cybercriminals to steal credit card information. Many large retailers have now rolled out systems compatible with Chip and PIN cards, bringing forth big security improvements to in-store payments.

All in all, 2015 was a year of new cybersecurity learnings and increased awareness. Yes, there were breaches. Yes, there were compromised accounts. But as we approach 2016, we have a better picture of where security stands across industries, and we are more prepared for what the New Year has in store for us. Until then, wishing you all merry New Year celebrations and online safety to boot.

Be sure to stay on top of the latest consumer and mobile security threats by following me and @IntelSec_Home on Twitter, and Like us on Facebook.

Tags: cybercrime, cybersecurity

Like 3 G+1 0 Tweet Email

No Comments

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

reCAPTCHA

Type the text

Privacy & Terms

Post Comment

Intel Security on Twitter

Security Need a hand optimizing your log-ins? We've got your back. https://t.co/KhFeTtgna7 #promo #SafeHoliday https://t.co/CC7Q4MunVZ

3 hours ago·Reply·Retweet·Favorite

elSecurity .@McAfee vanced Threat Defense protects against #fileless malware that drops a binary on its targets. Read on: https://t.co/v74IP88O2O

4 hours ago·Reply·Retweet·Favorite

Follow @IntelSecurity

Also Find Us On

About | Subscribe | Contact & Media Requests | Privacy Policy | Legal | FAQ