NORTON

Cyber Security Top Tips for 2016

2015 was a banner year for cybercriminals. We reported on 53 events that made it into the headlines, however that was just what we reported. There were many more than that occurred.

We took a look at what was trending to try to predict the next “big things” in cyber security to be on the lookout for in 2016.

1. **Ransomware:**
   Ransomware is the big topic this year. The first noticeable case of ransomware popped up in 2013, and hackers have latched on to this tactic, refining it over the years. In 2015 we reported on six major ransomware campaigns, which ranged from Mac to Android. Since ransomware can technically be performed on all device platforms, we expect to see a surge in these campaigns. Whatever happens, do NOT pay the ransom, and be sure to keep regular backups to help defend against these attacks.

2. **Fake Support Scams:**
   We saw increasing reports about tech support scams. Scammers use social engineering tactics in order to try to trick you into downloading malware onto your computer. They can come via a phone call from someone who claims to be from a tech support company stating that they have found a

problem on your computer. Internet pop-up ads can also be a source of this scam. They usually display a message stating that the computer is infected and offer a phone number for help with removing the malware. Often, these pop-ups will look like they come from a legitimate source, such as our own Norton products. Just remember, anyone contacting you asking you for money or access to your computer is a red flag.

Data Breaches:

Unfortunately, data breaches are becoming almost as common as malware outbreaks. We reported on 16 events, from large institutions to small. And this isn't just credit card fraud. Big data is big money for attackers, so they set their sights on companies that tend to hold large amounts of personally identifiable data on their customers, such as Social Security numbers, dates of birth, home addresses and even medical records. It's easy for a cybercrime victim to report credit card fraud and just get a new number. When it comes to Social Security numbers, you are bound to it for life. And Social Security numbers open the door to all sorts of identity theft.

3. **Software Vulnerabilities and Software Updates:**
   Major software vulnerabilities hit big in 2015. Attackers heavily rely upon these vulnerabilities, as it is the easiest way to sneak malware into a user's device unnoticed, with little action on the user's part. The best way to combat against these attacks is to perform any and all software updates as soon as they are available. Software updates perform a myriad of tasks to the program they are updating, such as patching those security holes attackers exploit, add new features and improve bug fixes. Recently, Microsoft announced their ending of support for Internet Explorer versions 7, 8, 9 and 10. Ending support means the end of software updates, so it is likely that many users may be migrating to the new Windows 10 for access to the new Edge browser.

4. **Windows 10 and Migration:**
   In addition to these hot topics, another one that was of noticeable interest was the Windows 10 release. In 2015, Microsoft offered up its operating system for free for the first time, either for old devices or installing them on new ones.