Security Awareness /Trends
August '16

CYBERSECURITY CONFERENCES

Cybersecurity Conference Update: Black Hat and Def Con

So what are Black Hat and Def Con anyway?

Black Hat and Def Con are the world's best known 'hacker conventions'. These conferences attract some of the world's best cyber security researchers and hackers. Where Def Con has typically drawn the more fringe elements of cybersecurity, Black Hat is its commercial counterpart and appeals to more mainstream security professionals. As these events draw near, rumors of new threats and vulnerabilities usually proceed them.

Notable Topics

To keep up on the latest threats impacting technology and privacy, following the speaker list and agenda is a must. The topic highlights this year included USB devices that could take control of a computer if inserted by an unsuspecting victim, machine learning, a type of artificial intelligence, is being used to improve the already successful spear phishing campaigns, and a demonstration that proved even the newly adopted credit cards with chip technology could be skimmed for information.

A Closer look at the Good and the Bad

While we're familiar with using the College Wi-Fi network how do we know we're actually on the College network? You would think the last place someone could be fooled into connecting to a malicious hotspot would be at a security conference. This year at Black Hat a security vendor monitored users connecting to what is referred to as an "Evil Twin". An Evil Twin is a hotspot that is controlled by an attacker with the same name as a legitimate hotspot. If your device joins this "Evil Twin" network, the attacker now has control of your network connection and can intercept data, manipulate network traffic and launch other remote attacks against you.

So how can you detect and protect against these types of attacks? Disable the auto-connect feature for saved hotspots. This is an option where your device can reconnect to a hotspot with the same name in the future without needing your acceptance. Out of date and bad security certificates are another warning sign that you are probably on an untrusted network. Another red flag would be the inability to use your VPN client. The attacker may be doing this to force you to use an insecure connection.

Keeping Safe Online

If you are one of the millions of iPhone users a significant update was released just days ago (Aug 25). Apple is urging its users to update their iPhone after serious security flaws were found. The flaws were discovered by security firms that were researching a suspicious text message. Clicking a link in the text would have infected the device with malware capable of reading text messages, emails, track calls, remotely record sound and collect passwords. In response, Apple released a patched version of its mobile software, iOS 9.3.5. Users can get the patch through normal software updates. If you're unsure what version you're running, you can check Settings > General > About > Version.

Apple recently launched a bug bounty program to encourage responsible disclosure for discovered vulnerabilities. Bug bounties are cash awards (Apple is offering $200,000) offered by vendors to individuals for finding a software bug and reporting it.