Security Awareness / Trends September '16

PRIVACY AND TRUST

Privacy and Trust

Social Information Sharing

How do you decide to share personal information online? If you're like most people, there's a tradeoff between sharing your personal information and getting something valuable in return. The value may come from a retail loyalty card that tracks purchase history in exchange for discounts, a smart thermostat that monitors your movement in your home to lower your utility bills, or a new financial app to track transactions and your budget while trending spending habits. What shapes many of our opinions to share or not to share is our comfort level with the company and how trustworthy we perceive them to be.

If you choose to share, be certain you understand the fine print. What happens to the data after it is collected? Is the data made available to a third party and how long does the third party keep your information? We've seen them, but how many read the terms of service before we install an app or join a service? If you use Twitter, then you have agreed to grant them the rights to all your content. Purchases made in iTunes do not provide ownership of the media, merely the rights to watch and listen to that media. Netflix reserves the right to disclose information to third parties and will not be held liable if it gets hacked and personal information is stolen. So, before clicking the agree button, do a quick search to see what others have said about a company's terms of service.

Trust in the Cloud

Cloud services and the Internet of Things are transforming how we conduct our business and is turning our data into a form of currency. JCCC's responsibility is to manage the volume, variety and sources of this data as we make the move to the cloud. During the move to the cloud, we have been very deliberate to evaluate the access controls and policies available within a cloud service to effectively prevent data leaks or unauthorized access. As an example, Microsoft OneDrive allows us to audit shares that are shared externally. Microsoft has also increased its data loss prevention (DLP) tools to allow tagging of data. Data that is tagged restricted, sensitive or public based on its content can be treated accordingly by cloud applications. As an example, data tagged as *restricted* could be denied the ability to be shared outside JCCC. Users of certain Office 365 applications may see this functionality enabled as early as this fall.

Education Top Target for Ransomware

Ransomware continues to increase, doubling and tripling in reported incidents in the past year. The FBI sees the rise in ransomware as a result of victims electing to pay the attackers in exchange for their data (InfraGard 2016). This only encourages attackers to continue and extort the next person. A recent report by BitSight (Murnance 2016) found that educational institutions like JCCC are the top target for ransomware, followed by government, healthcare, utilities, retail and finance. This may be due to education's open culture and complex user environments. To protect JCCC, we secure the network to block known bad URLs and sites, we update virus definition files nightly to protect workstations, and backup critical data. Email and malicious web sites are still the biggest threats. As users, we need to be suspicious of emails with attachments and embedded links. If you are concerned about an email you can report it for review to spamreport@jccc.edu

InfraGard, https://www.infragard.org (accessed Aug. 2016)
Kevin Murnance, "The Rising Face of Cyber Crime: Ransomware", Sept. 2016, https://info.bitsighttech.com/bitsight-insights-ransomware