Webinar Questions and Answers

Cybersecurity Awareness Updates

Webinar guests submitted several questions before and during the **25 June 2015, Cybersecurity Awareness Update** session. The following responses are provided by the Center for Development of Security Excellence (CDSE):

Question: What is OPM doing to mitigate future breaches? Are there any outside agencies, other than IG, assisting OPM and other federal agencies that have had audits indicating badly needed upgrades to network infrastructure to protect information?

Answer: OPM has released a statement about the measures they're taking to protect user data in the future: https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/.

Question: We have members that have received an email from an OPM site in regards to the most recent hack. They were informed on the link that the pin code was required and they needed to provide their social security number and other PII.

Answer: OPM did send out messages to that effect; however, they changed their notification due to recipient concerns.

Question: How secure are QR Codes that are use at the airport for airline ticket?

Answer: QR codes do have a useful purpose, which has to be balanced with the security risks of using them. In the case of airline tickets, I would consider that to be a trusted source. Generally speaking, you can see them being printed and you maintain control of the ticket throughout the process.

In most cases, if not all (I haven't personally seen an exception), it's the airline that scans the QR codes on the tickets. The system they're using has a singular purpose, which is to read the flight information. A QR code that redirects to a web page, for example, shouldn't be able to do anything to their system. Of course there may be exceptions depending on the equipment and configuration of the equipment.

Question: What do you think could've been done to prevent the attack with OPM Personnel Record?

Answer: OPM has released a statement about the measures that they're taking to protect user data in the future: https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/.

Webinar Questions and Answers

Question: Can you explain Two Factor Authentication Email?

Answer: Two-factor authentication, as it relates to email, means that you need two things to log in. Depending on your preference, you can require those two things every time you log in, or just every time you log in from a new location (that's what I personally use). One of those things is probably going to be your password, but you can also have a text message sent with an additional code. That way, if your password is compromised, the attacker would also need your phone in order to compromise your email.

Many email systems, such as Gmail, have two-factor authentication as an available option in the settings.

Question: What do you think of the recent hack into cleared personnel information?

Answer: OPM has released a statement about the measures that they're taking to protect user data in the future: https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/.

Question: How do we protect ourselves when large companies such as Home Depot, IRS, etc. get hacked?

Answer: When we entrust our financial and personal information to a company, we rely on them to protect it. Unfortunately, sometimes those companies get compromised and our information can be released. Should that happen, it's important to monitor your credit report and banking information, and take advantage of fraud protection services through trusted third parties or your financial institution. Canceling affected bank or credit cards and changing passwords can help to avoid problems that may stem from the breach.

Question: What about JAVA?

Answer: Current vulnerabilities and information about specific technologies not addressed in the brief can be found on US-CERT's website at https://www.us-cert.gov/ncas/bulletins.

Question: Android issues?

Answer: Current vulnerabilities and information about specific technologies not addressed in the brief can be found on US-CERT's website at https://www.us-cert.gov/ncas/bulletins.

Question: What about Virus Scanner Trust - Regarding Kaspersky and their "hack?"

Answer: Current vulnerabilities and information about specific technologies not addressed in the brief can be found on US-CERT's website at https://www.us-cert.gov/ncas/bulletins.

Webinar Questions and Answers

Question: Any additional info on the OPM hack?

Answer: OPM has released a statement about the measures that they're taking to protect user data in the future: https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/.

Question: Any suggestions on hardware-level hacks like the USB Firmware vulnerability?

Answer: In many cases, patches and updates to a system's firmware may help remediate hardware-based vulnerabilities; however, the USB firmware vulnerability is one example of a case where no patch or update could remediate it. The USB ports could be disabled through settings, as well as software or physical configuration, but that's not always ideal. In that case, effectively training users and informing them of the policy is a course of action that could help protect a system.