Deputy Download

October was Cybersecurity Awareness month, and of course, while having a month to focus on the importance of cybersecurity is a fantastic opportunity, we all have to be security aware throughout the year. Cyber attackers have grown more sophisticated and will take every advantage they can to abuse trust to further their means, whether the goal is to steal sensitive information, disrupt critical services or misuse government trust and resources for their own purposes.

Phishing of credentials is the number one threat to state government systems today. Only provide your login user name and password to the application you expect to be using. It pays to check the website address before you enter your credentials just to be certain. Never provide your logon information as a response to a link in an email that you did not solicit, as you might with a username or password reset that you initiate. And never send your username and password in an email to anyone! Our helpdesks will never ask you to do this.

ESO is working to develop some recommendations, based on industry best practices, for agencies to implement practices to help protect our email systems. However, the best protection for the state by far is a security aware workforce that helps protect our systems and data from cyber criminals.

If you have suspicions about whether an email is legitimate or not, please contact your agency’s supporting IT service provider, or the ESO SOC Malicious Helpdesk. The Helpdesk can be reached at 503-378-5930 or at eso.soc@oregon.gov.

Training and Awareness

October was National Cybersecurity Awareness Month, also referred to as NCSAM. Now in its 15th year, this annual, nationwide campaign is a collaborative effort between government and industry designed to raise awareness about the importance of cybersecurity and to ensure every individual has resources to help them stay safer and more secure online.

To help with this effort, ESO added various cybersecurity resources to its public facing website, such as newsletters, tips and advice, games, and resources dedicated for parents and kids. ESO also created a calendar of events page to help spread the word about local training, webinars and more. Read the Governor’s proclamation on Cybersecurity Awareness Month at oregon.gov/das/oscio/documents/2018cybersecurityawarenessmonthproclamation.pdf.
SOCed In

Women in information security

At my time leading the Security Operations Center, I’ve been fortunate to work with Aimee Whitney. Aimee is a Security Operations Center (SOC) Analyst and one of 21 women that are part of the Enterprise Security Office. At close to 40%, we are proud that ESO has nearly four times the nation-wide average of women in information security. While I am proud of this representation within the state government information security community, I understand that this is the exception. Over the past two years, the number of women in the information security field has dropped to about 10%. And, of the candidate pools I have worked with during that same time period, women have been significantly underrepresented.

I constantly encourage women and minorities to pursue a career in information security. Not sure if that’s your thing? Do you know someone who might want to know more? Read “The Cuckoo’s Egg” by Cliff Stoll and see if that captures your imagination. His story has inspired countless people to pursue the profession of information security. It’s a true story from the 1980s with information security principles that are just as relevant today…and it’s a fun read. If this piques your curiosity, follow up with a free online course at chrissanders.org/training/cuckoosegg/. The course is designed to provide an introduction to information security, as told through the lens of the book.

Shawn’s Services

The term firewall originally referred to a wall intended to confine a fire within a building. Later uses referred to similar structures, such as the metal sheet separating the engine compartment of a vehicle or aircraft from the passenger compartment. The term was applied in the late 1980s to network technology that emerged when the internet was fairly new in terms of its global use and connectivity. The predecessors to firewalls for network security were the routers used in the late 1980s.

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the internet.

The Enterprise Security Office currently manages, maintains, and supports over 100 individual network firewall devices across state government.

Kristine’s Korner

According to the CIS Controls FAQ, “CIS Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to thwart the most pervasive attacks. The CIS Controls are a relatively short list of high-priority, highly effective defensive actions that provide a ‘must-do, do-first’ starting point for every enterprise seeking to improve their cyber defense.”

Because the State Chief Information Security Officer has identified the CIS Basic 6 Controls as the minimum requirements for agency compliance, ESO has identified 33 of the 47 sub-controls within the Basic 6 Controls as ‘primary controls’ – these are controls that agencies must, at a minimum, implement. Oftentimes, though, thoughts of implementation immediately turn to technical solutions. And technical solutions can be an answer. However, complete implementation also requires a thorough understanding and documentation of standards and workflows – e.g., roles and responsibilities, processes or procedures, and reporting to the business. This is what differentiates Enterprise Architecture from ad-hoc solutions. To be continued….
IT Security Contracts

The Enterprise Security Office launched National Cyber Security Awareness Month with a Security Services Kickoff on October 2. ESO partnered with DAS Procurement Services and OSCIO Basecamp for the event. Attendees received information on a broad array of topics including security initiatives, security service master agreements, and the procurement process. There was also an in-depth discussion on how to use agreements, with special insight into vendor management.

ESO’s mission is to provide broad security support not only to state agencies, but to the whole of Oregon. The event showcased a major move in that direction. The master agreement is now widely available to the Oregon Cooperative Procurement Program, along with state agencies. ORCPP’s membership includes local governments, education, tribal, and special districts. This puts security support services in the hands of thousands of Oregonians across the state.

Video of the event will be available on ESO’s website. While you’re there, take a moment to check out our security tips and advice, along with contact information for our office.

Stay Cyber-Safe this Holiday Season

During the holiday season, millions of people will place orders online. Cybercriminals take advantage of this increase in online activity in many ways. Here are some tips to help protect you and your family.

Look for https://
Before you enter any information, look for an “s” at the end of “http” on the web address payment page (the URL should start with “https”). The “s” stands for a secure connection.

Use one card for online purchases
Try using a single card for online purchases and a different one for in-store purchases.

Beware of phishing emails
Phishing increases during the holiday season. Popular phishing email themes revolve around invoices, gift cards, delivery notifications and special deals. Double check the email address and don’t click on unknown links or attachments in the message. Keep a list of what you order and the shipping method used for quick reference.

Watch out for holiday SMiShing
“SMiShing” is like phishing, only through text message. Watch out for scammers trying to lure you in to giving up your personal information or unknowingly downloading a virus or other malware onto your cell phone or other mobile device.

Scrutinize freebies on social media
“Free” iPads, flights, movie tickets and cheap Ray-Ban sunglasses all fall into the category of “if it looks too good to be true, it probably is.”

Beware of malicious mobile apps
Beware of the apps you download. Scammers like to create fake, malicious shopping apps designed to steal your information.
Puzzles
What's wrong with this picture? There are 15 things not right—how many can you find?
Check in next month for the answers!

Last Month’s Answers
Vulnerability
Cloud Exploit
Inventory Standard
Scanning Tenable

The final answer? “Security Depends on You!”