Awareness Primer

Table 2. *Virtual CySecEscape 2.0—Awareness topics and related puzzles.*

Awareness topic	*Puzzle*
Physical security	Unclean desk contains hints about login credentials.
Password hygiene	Easy-to-guess password.
Source code security	Source code evaluation (“hidden path”).
Information disposal	Bank account data in trash.
Securing sensitive digital data	Password reuse on sensitive file.
Public oversharing/identity theft	The missing employee is found through social media, then turns out to be impersonated.
Phishing and online banking	Phishing mail causes loss of access to bank account (game ends).

Physical security Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism. While most of these are covered by insurance, physical security's prioritization of damage prevention avoids the time, money and resources lost because of these events.

Password hygiene refers to the degree to which a user's passwords are selected and managed according to secure best practices. The practices important for good password hygiene include, but are not limited to, selecting passwords that are not obvious, perfunctory, or common, selecting a unique password for each account, avoiding the temptation to write passwords for easy recall, and avoiding the temptation to share passwords with others for convenience. Bad password hygiene is responsible for countless data breaches and individual account takeovers, and security administrators routinely invest time and effort to educate users about bad password hygiene and its consequences.

Source code security is a collective term for actions aiming at securing your code. In the past few years, efforts to compromise devices, apps, and software have surged as the rewards can be highly valuable. Source code plays a critical role in building applications, making it crucial proprietary information. Your source code can contain secrets, such as API or encryption keys, OAuth tokens, passwords, and more. It is also common for personally identifiable information (PII) to coexist with source code. Without protection, these are available to all repository contributors meaning that they can clone, copy, and distribute them. Actions include protecting the security of source code and other sensitive data even when employees work remotely away from your network or when offline, or control and block the transfer of source code through instant messaging apps, email, cloud storage services, file-sharing services, and more to avoid data loss.

Secure **information disposal** is especially important for classified material, where one wants to ensure proper data disposal to prevent unauthorized access. The law requires that computers, electronic devices, and media be erased and/or disposed of properly to safeguard sensitive data. Anything with a hard drive or external storage containing sensitive data such as laptops, printers, copy machines, faxes, USB drives, external hard drives, CDs and DVDs, tapes, and workstations must be properly destroyed. Physically destroy the device. One popular method for doing this is by shredding the device. Actions include to have information (e.g. paper) professionally shredded for proper data disposal, or wiping devices like hard drives with special software, rendering sensitive data unrecoverable or, at the very least, unreadable.

Securing sensitive digital data includes having an understanding where sensitive data resides, having set policies in place to systematically and consistently categorize the data, and consequently, have controls in place to ensure that all categories of data are handled appropriately. For example, access to payroll data is usually restricted to those employees that process the payroll and those that review it. This is usually done within a payroll application that has built-in security and access controls (e.g., SAP). Payroll data and similar data sets should NEVER be downloaded onto an unsecure laptop, thereby undermining all the required controls.

Public oversharing/identity theft stands for providing your personal information online, and enabling social engineer to abuse that information. Many consumers are sharing some of their most sensitive personal information on social networks, which includes sharing personal details that could put them at risk for fraud and identity theft. Once a digital identity or at least its part falls into the hands of criminals, it can be abused in a multitude of ways: it can be resold, it can be used for blackmail, for money, your "digital identity" can attempt financial or medical fraud. This includes seemingly unimportant information such as sharing your birthday date on LinkedIn, as this is often a security question to identify you when calling your bank.

Phishing and online banking are related terms. Phishing attacks come from scammers disguised as trustworthy sources and can facilitate access to all types of sensitive data, among others the online banking. As technologies evolve, so do cyberattacks. There are different forms of phising, a few are stated in the following. When bad actors target a “big fish” like a business executive or celebrity, it’s called whaling. These scammers often conduct considerable research into their targets to find an opportune moment to steal login credentials or other sensitive information. If you have a lot to lose, whaling attackers have a lot to gain. The most common form of phishing, this type of attack uses tactics like phony hyperlinks to lure email recipients into sharing their personal information. Attackers often masquerade as a large account provider like Microsoft or Google, or even a coworker. Where most phishing attacks cast a wide net, spear phishing targets specific individuals by exploiting information gathered through research into their jobs and social lives. These attacks are highly customized, making them particularly effective at bypassing basic cybersecurity. See public oversharing/identity theft as a precondition for spear phishing.