# Risk Descriptions

The following are the different risks you can select for the purpose of your lab. We not only describe each risk but also the behaviors that are taught to manage the risk.

Phishing (\*ishing)

Phishing is one of the most common (and often one of the most effective) types of social engineering attacks. By “phishing,” we mean not only email-based phishing attacks but also messaging-based attacks (smishing) and voice-based attacks (vishing). This module explains not only what these attacks are and why they are so dangerous but also the most common indicators and the importance of reporting.

Browsing

The browser has become the gateway to the internet; it is the primary tool that employees use for online activity. As such, browsers and their plugins have become a common target for attackers. We teach people how to browse safely, including keeping the browser and plugins updated, ensuring people do not synch their personal browser accounts with their work browser, how to react when they see a warning banner, and being careful of and scanning files they download.

Social Media

Websites and mobile apps such as TikTok, Twitter, Snapchat, and LinkedIn have exploded in popularity, with employees and managers posting all sorts of private information, not only about themselves but also about their work. Cyber attackers know this and use social media for identity theft, spreading scams and malware, and harvesting data for targeted social engineering attacks. We discuss these risks and the steps your workforce can take to protect themselves and your organization.

**Working Remotely**

You are concerned about people working way from the office, either at home or on the road. While many of the security issues are the same (use of strong passwords, watching out for social engineering attacks, etc.), there are also unique risks. For example, ensuring people do not lose or forget their devices, ensuring non-authorized individuals (strangers, children, etc.) do not access devices, and perhaps ensuring that employees use VPNs when traveling.

Mobile Devices

Today’s mobile devices (such as tablets and smartphones) are extremely powerful. In most cases, these devices have the same functionality, complexity, and risks as a computer, but with the additional risk of being highly mobile and easy to lose. We cover how to use mobile devices safely and how to protect the data on them, focusing on screenlocks, updates, and the use of trusted mobile apps only.

Passwords

Passwords are the keys to the kingdom, and employees must guard them well. Risks include cyber attackers easily guessing, cracking, or harvesting and using legitimate credentials. We cover what passwords are, why they are important, and what makes a strong password, with an emphasis on passphrases. In addition, we cover how to protect and safely use passwords, including the use of unique passwords for every account, password managers, and multi-factor authentication.

Data Handling

Organizations have a tremendous amount of sensitive information that they must take extra steps to protect. This module explains these steps, focusing on how to identify sensitive information, using only authorized systems to store or process sensitive information, restrictions on transferring or sharing such information, and requirements for securely disposing of sensitive data.

**Cloud**

The cloud is a powerful tool that enables your employees to increase their productivity while reducing organizational costs. However, it also comes with tremendous risks. This module focuses on what organizational data can be stored in the cloud, which cloud providers can be used, and how the data should be securely shared with others.

**Detection and Incident Reporting**

We are not only developing the human firewall but the human sensor. We are at risk if people are not reporting incidents, such as infected systems, suspected attacks, and lost devices. This module teaches people how to identify an incident, how to report an incident, the importance of reporting, and how there will be no negative repercussions or punishment even if they caused the incident. We want to ensure people not only know how to report an incident but feel safe reporting.