|  |  |
| --- | --- |
| Phishing  1a. The answers | A fraudulent email or text message disguised as a legitimate email, often claiming to be from a trusted source. The message is meant to trick the recipient into sharing personal or financial information or clicking on a link that installs malware.  1b. to four of |
| Spear phishing  2a. the quiz | A targeted attack via email on specific individuals or enterprises with a tailored message based on characteristics, job positions, and contacts belonging to the recipient to make the attack less obvious. This attack is harder to detect and has a higher success rate when done skillfully.  2b. questions reveal |
| Whaling  3a. the words that | An email or website that targets senior management who have complete access to sensitive data. The goal is to trick an executive into revealing personal or corporate data.  3b. can be turned |
| Vishing  4a. into the single-digit | The use of social engineering over the phone to gather personal and financial information from the target.  4b. numbers that are |
| Tailgating  5a. needed for the | The act of gaining entry into a secured building by following someone with an access card. The unauthorized individual may pretend to be a delivery person, visitor, student, or employee.  5b. 4-digit combination |
| Impersonation  6a. lock. Convert each | Practice of pretending to be someone else with the goal of obtaining information or access. Can be done over the phone, in person or via e-mail. Best technique used by social engineers because people want to be helpful.  6b. of the four |
| Dumpster diving  7a. answers into | The act of searching through trash to gather sensitive information. Improperly discarded documents can provide a huge amount of material that can even be used to impersonate an employee.  7b. numbers. Add the |
| Shoulder surfing  8a. digits of each | Perpetrator gains access to sensitive information by watching what you are typing, viewing the screen, or simply eavesdropping on phone calls or conversations.  8b. answer until you |
| Baiting  9a. get a single-digit | The act of leaving USB devices in parking lots or the waiting area of airports in the hopes that a person will find it and insert it into a computer to see what is on the drive. It can then automatically install malware, ransomware or a virus on the device.  It can also be in the form of an enticing ad or email that leads to a malicious site or that encourages users to download malware.  9b. number. Find |
| Scareware  10a. the vertical | Tricking a person into thinking their computer is infected with malware or has inadvertently downloaded illegal content. Then the attacker offers a downloadable solution to fix the bogus problem but in reality, installs malware. Can appear in the form of a popup banner or via spam email.  10b. clue that |
| Smishing  11a. reveals the | The use of SMS texts sent to a mobile phone to initiate a scam. The goal is for the target to log onto a fake website with their smartphone, and download malicious code that could give the hacker access to anything on the phone.  11b. four correct |
| Surveys  12a. quiz answers and | Attempt to gather information online, via telephone or in person. May be for legitimate purposes or it might be a scam. In either case, be aware of unwittingly disclosing information that may be used inappropriately.  12b. the lock order. |
| What has a head and a tail but no body?  -- | Wich  -- |
| If you have me, you want to share me. If you share me, you haven't got me. What am I?  -- | Mywlyn  -- |