**LUCY Social Networking Storyboard**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr** | **Graphic** | **English** |  |
|  |  |  |  |
|  |  | This LUCY video will teach you to identify the many forms of social engineering and their potential impact. |  |
|  |  | So what is social engineering? |  |
|  |  | Social engineering is a manipulative strategy where cyber attackers try to trick you into sharing confidential information or letting them into restricted zone in your organization. |  |
|  |  | Some examples include:  Using someone else’s pass to enter company premises  Posing as maintenance or IT or auditor to get into company premises. |  |
|  |  | Social engineering could be conducted face to face, over the phone or via email or social media. |  |
|  |  | Cold calling is a technique where the attacker dials random numbers within the company, pretending to be IT or maintenance calling about an issue. |  |
|  |  | Eventually, they might happen upon somebody with an issue who might pass them their login credentials or other company information. |  |
|  |  | Shoulder surfing uses direct observation to steal personal information. |  |
|  |  | It is best employed in crowded areas where it’s easy to look over someone’s shoulder and see their PIN number or information they fill into administration forms. |  |
|  |  | Information we share in our social media profile and posts can be easily used by attackers who pose as our friends. |  |
|  |  | Baiting technique lure users to share their online credentials with a promise for free downloads or other goods, but they’re not limited to online schemes. |  |
|  |  | Attackers might leave a USB drive or CD in visible locations counting on human curiosity to lure someone into loading the drive. |  |
|  |  | Usually, such external memory drives are used to carry malware that infects the victim’s system. |  |
|  |  | Phishing scams are very popular. |  |
|  |  | They trick the victim into sharing their personal, financial or login information or to unknowingly download malware to their computer. |  |
|  |  | The usual medium is emails, but social media, phone calls, chat applications and spoofed websites are commonly used. |  |
|  |  | Pretexting is a technique where the attacker builds a false sense of trust with the victim. |  |
|  |  | They create a credible story (IT auditor/maintenance crew, etc.) that gives them the opportunity to get on the company premises or to gain valuable information about the organization. |  |
|  |  | So how do we protect ourselves from social engineering attacks? |  |
|  |  | **Tip #1**  Be suspicious of any unsolicited messages. |  |
|  |  | Do not open suspicious emails until you verify via phone call or personal interaction with the sender that the message is legit. |  |
|  |  | **Tip #2**  Beware what you share! |  |
|  |  | Any information you post online can become available to all internet users – from your birthdate, to your occupation, vacation habits, etc. |  |
|  |  | Social engineers use that information to profile you and create an attack tailored just for you. |  |
|  |  | **Tip #3**  Don’t share any personal or company data before you verify the identity of the person asking and the reason they need the data. |  |
|  |  | **Tip #4**  Secure all your computing devices with anti-virus software, firewalls and e-mail filters and keep those up to date. |  |
|  |  | **Tip #5**  Be careful what information you disclose to people. |  |
|  |  | Always be suspicious of characters you don’t know, especially if they ask questions that don’t fit their persona (your vacation plans, operating system, etc.) |  |
|  |  | **Tip #6**  Always consider your setting when you are using your devices. |  |
|  |  | Look around and choose a location that will prevent shoulder surfing. |  |
|  |  | And never login to your accounts or transmit personal or company data over public, unprotected networks. |  |
|  |  | **Tip #7**  Unescorted visitors pose threat to any organization. |  |
|  |  | Should you see such a person, make sure you help them get where they claim they are going.  Then notify security about them. |  |
|  |  | Never let anyone borrow your access card, and do not leave visitors alone with sensitive information. |  |
|  |  | If you suspect a social engineering attack:  Report the incident immediately. |  |
|  |  | Share your suspicions with others. |  |
|  |  | Follow company security policies. |  |
|  |  | DO NOT assume you can trust everyone. |  |
|  |  | Stay calm and friendly without providing any personal or company information. |  |
|  |  | Contact your financial institution and monitor your account activity. |  |
|  |  | Change all your passwords. |  |
|  |  | Thank you for watching and reminder:  Security is everyone’s job.  Please take it seriously. |  |