Jahnke (0808831)

CSCI 289, Fall 2022 (Online)

Assignment IV

1. Yes, hiring former hackers to enhance security is a good idea. Two reasons:
   1. High-caliber former “black hat” hackers can be a wealth of knowledge. They may know of techniques “white hat” hackers would have never thought of or could not explore due to legal or ethical concerns. To defeat a malicious hacker, you need to think like a hacker. Who better than someone who’s done it? So, if companies are looking for top-notch cybersecurity, hiring former “black hats” may give them an edge in the market…assuming the person has been rehabilitated.
   2. Some hackers hack because they “have an itch”. The thrill of the hunt is what gets their juices flowing and they’re going to want to hack no matter what comes their way. Offering them a job can be viewed as giving them the opportunity to use their talents for good (finding the guys who hacked into a system) than for ill (being the guys who hacked into the system). If they’re going to do it anyway, why not give them the chance to be “the good guys”?
2. Two suggestions for resolving issues created by differences in laws between different countries:
   1. Promote the authority-to-prevent-entry principle on the international stage. I agree with this principle as it allows each country to maintain its sovereignty. If implemented, less resources may be utilized to preemptively build cases against foreign companies or citizens who can only be tried if they cross into the border of that country. Private companies (if they so desire) can work with nation-state governments to set up specialized versions of their services to fit the law of that country. Otherwise, the company can operate under the laws and regulations of the country in which they are headquartered, thus allowing them to operate freely with less fear of charges being brought against it due to some obscure foreign law.
   2. Establish an international body that determines the best practices for operations in cyberspace. Each nation may send representatives to make pleas for certain policies, debate other policies, and raise questions. The body may establish certain standards and individual countries could make commitments to those policies. This may increase cybersecurity measures and training for developing countries. The body may help to iron out some of differences in applicable cyberspace laws between countries so that litigation costs go down and efficiency increases for all members involved. The body may enable a common defense against adversarial countries who operate with malicious intent in cyberspace.
3. Two techniques criminals can use to gather information used to steal identities:
   1. Criminals can scour job-hunting websites to gather information to help them build a profile of a target they can then use to impersonate the target. This information may include addresses, work histories, birth dates, and maybe even likes and interests. They may post fake job listings and ask probing questions to respondents claiming that the information collected is part of a background check.
   2. Criminals can sit in locations with unsecure public Wi-Fi, such as cafes or restaurants. With the right tools, they can infiltrate a network and monitor the traffic going through it. They could then inject viruses or spyware onto they devices of other users. Once that happens, the other devices become the hackers’ devices.
4. Two ways business can protect its customers from identity thieves:
   1. Monitor spending habits of customers and the geolocations from where purchases are made. If an exceptionally unusual or high-ticket purchase is made or if transactions are being processed from odd places in the world, ask for verification from the customer.
   2. Add an additional layer to the login and/or purchasing process to verify that the purchase request is coming from a human (e.g., CAPTCHA, “pick-the-photo-with-the-penguin” tests, one-time-use verification PINs via text or email).
5. Two ways a person can protect their identity:
   1. Use strong passwords, update them frequently, and don’t use the same password for different services.
   2. Opt-in to using multifactor authentication methods for the services used to mitigate the opportunity for hackers to use your login credentials without your knowledge.