Headline: Cybertheft growing concern worldwide

Deckhead: Turn to AAA to take proactive approach to stop villains

Few things are more important than protecting our identities. Our personally identifiable information (PII) rests on the internet waiting to be plundered.

Cyberthieves work around the clock, searching for ways to infiltrate our com­puters. Cybertheft is expected to cost the world $13.8 trillion by 2028.

October is recognized as National Cybersecurity Awareness Month. The U.S. Department of Homeland Security and the National Cyber Security Alliance collaborated to create this endeavor as a time to remind and inform individuals on the importance of protecting their PII from cybercriminals.

It’s an enormous task, considering no amount of knowledge is guaranteed to keep information safe from cyberthieves. It’s not *if*, but *when* a cyberattack occurs, how can a person limit the effect caused by the damages?

The best defense is to not make it so easy for a hacker to steal PII. Using strong passwords is essential. Passwords should have multiple characters, upper- and lower-case letters, numbers and symbols. The longer the better. Avoid using birthdates or anniversary dates. Don’t capitalize the first letter without capitalizing others within the password.

Never write passwords on a sheet of paper, use the same one for multiple sites or give them to another person. Avoid typing a password in an office setting without making sure another person isn’t standing in the background. Shoulder surfing is a common method used by hackers to steal passwords.

Two-factor authentication decreases the odds of a password being stolen, and password generators can randomly produce words that could take as long as three centuries to crack.

Email is another concern. Phishing emails can be difficult to identify and are meant to steal PII or hold the computer hostage. A hacker can lock a computer and its information until a monetary demand is met, but even then, there is no guarantee the information will be returned once the ransom is paid.

It’s good practice to closely read the addresses from which emails are being sent if they seem suspicious. A message might read that it was sent by Microsoft, but there could be mis­spellings in the address – a primary red flag. Does the message address the user personally or randomly? Messages beginning “Dear sir” or “To whom it may concern” are red flags. Poor gram­mar within the message is another red flag. Delete them immediately.

Maintaining updated antivirus soft­ware and using a firewall also are critical. Try to avoid visiting websites that have URL addresses beginning with “http” rather than “https.” The “s” indicates the site is secure, and it’s safe to visit. Following these steps can greatly reduce the odds of being hacked. PII in the wrong hands can steal a person’s iden­tity, ruin years of good credit or empty bank accounts.

ProtectMyID can help monitor a per­son’s identity for fraudulent activity, and fraud-resolution agents work to restore reputations. AAA memberships come with exclusive savings on identity-theft protection that include ProtectMyID Deluxe Coverage for $10.95 monthly, ProtectMyID Platinum Coverage for $15.95 monthly and the Complete Plan that costs $19.95 monthly for Members and $22.17 for non-Members. Limited features are available for free with ProtectMyID Essential.

Remember, no plan is guaranteed to keep a person fully protected. But *no* plan greatly increases the likelihood it will happen.

Take advantage of AAA’s identity-theft plans before a hacker takes advantage of you.

Cutline: STAY PROTECTED – Combatting cybertheft takes effort and well-planned strategy. Image: JJAVA. Adobe Stock.