Le phishing :

Le phishing est la pratique consistant à envoyer des e-mails frauduleux qui ressemblent à des e-mails provenant de sources fiables. L’objectif est de voler des données sensibles telles que des numéros de carte bancaire et des informations de connexion. C’est le type de cyberattaque le plus courant. Vous pouvez vous protéger grâce à l’éducation ou à une solution technologique qui filtre les e-mails malveillants.

Les ransomwares :

Les ransomwares constituent un type de logiciel malveillant. Ils sont conçus pour extorquer de l’argent en bloquant l’accès aux fichiers ou au système informatique jusqu’à ce que la rançon soit payée. Le paiement de la rançon ne garantit pas que les fichiers seront récupérés ou le système restauré.

Le malware :

Le programme malveillant est un type de logiciel qui permet d’obtenir un accès non autorisé ou de causer des dommages à un ordinateur.

L’ingénierie sociale :

L’ingénierie sociale est une tactique que les hackers utilisent pour vous inciter à révéler des informations sensibles. Ils peuvent solliciter un paiement ou accéder à vos données confidentielles. L’ingénierie sociale peut être combinée à l’une des menaces répertoriées ci-dessus pour vous rendre plus susceptibles de cliquer sur des liens, de télécharger des malwares ou de faire confiance à une source malveillante.