Chapter. 12 정보 보안

1. “**보안**”은 다양한 위협에서 **자신의 신체나 재산을 지키는 일체의 행위**를 의미한다.

2. **IT 분야**에서 보안 관련 기술은 “**물리보안**” 과 “**정보보안**”으로 나뉜다.

3. **수집하고 가공한 정보**를 **송수신 및 저장하는 과정에서 발생할 수 있는 훼손, 변조, 유출 등 불법적인 행위를 차단하는 방법**을 “**정보 보안**”이라고 정의 한다.

4. “**컴퓨터 바이러스**” 는 **컴퓨터 속의 자료를 없애거나 시스템을 정지하려고 만든 파괴적인 소프트웨어**로, **주변을 감염시키는 특징**이 있다.

5. ‘**컴퓨터 바이러스보다는 조금 약한 약성 소프트웨어’**로, 컴퓨터 바이러스와 달리 **자기복제 능력이 없는 소프트웨어**를 “**트로이목마**”라고 한다.

6. 엑셀, 워드 , 파워포인트 같은 **데이터 파일에 포함해서 배포**하는 악성 소프트웨어를 “**매크로 바이러스**”라고 한다.
   보통 악성 소프트웨어는 **실행 파일에 포함해서 배포**한다.

7. 감염되면 컴퓨터 내 모든 파일에 암호가 걸려 **돈을 받은 후에만 암호를 풀어 주는 악성 소프트웨어**를 “**랜섬웨어**” 라고 한다.

8. **인질범이 요구하는 몸값이라는 이라는 의미**로, 돈을 벌 수 있기 때문에 최근 유행하는 악성 소프트웨어는 “ **랜섬웨어**“ 이다.

9. 사용자 화면이나 웹 사이트 초기 화면에 **사용자 동의 없이 광고를 띄우는 소프트웨어**를 “**애드웨어(adware)**” 라고한다.

10. **사용자 동의 없이** 방문하는 웹 사이트, 사용 패턴, 개인정보 같은 **정보를 몰래 훔쳐 가는 프로그램**을 “**스파이웨어(spyware)**”라고 한다.

11. **악성 소프트웨어**는 사용자 실수로 **시스템에 침투하여 불법 행위**를 일으키는 데 반하여, “ **크래킹” 혹은 “해킹**“은 **시스템 외부에서 침투하려는 모든 시도**를 가리킨다.

12. **좀피 컴퓨터 여러 대**에서 **엄청난 양의 데이터를 서버로 보냄**으로써 다른사람이 서버를 이용하지 못하게 하는 해킹 방법을 “**디도스**” 공격이라고 한다.

13. **네트워크로 전송되는 데이터를 검사**하여, 악성 소프트웨어나 해킹이 **내부로 침투하지 못하게 막는 소프트웨어**를 “**방화벽**“ 이라고 한다.
시스템 내부에 있는 정보가 불법적으로 외부로 나가지 못하게 막는 기술도 포함한다.

14. **사용자가 본인임을 입증하는 가장 기본적인 방법**으로, 숫자와 문자를 조합하여 만든 것은 “**패스워드**”이다

15. 일정 시간만 쓰고 버리는 패스워드를 “**OTP (One Time Password)** 라고 한다.

16. 지문 인식, 안면 인식 , 행채 인식처럼 **신체를 이용하여 인증**하는 것을 “**바이오**“ 인증이라고 한다.

17. **공인된 기관에서 인증**한 전자서명을 “**공인인증서**”라고 한다.

18. **디지털 콘테츠**를 **무단으로 유통하고 사용하는 것을 막는 방지 기술**을 “ **DRM (Digital Rights Management)**“라고 한다. 디지털 권리 관리 기술

19. 불법적으로 도용되었을 때 **자신이 찍은 사진이나 그림이라는 것을 증명할 수 있는 기술**을 “**워터마크**”라고 한다.

20. 암호화 기술에서 하나의 키로 암호화 혹은 복호화하는 방식을 “**대칭** “ 혹은 **단일키 함호화** 라고 한다.

21. **단일키(대칭) 암호화 방식의 가장 큰 단점**은 암호로 만든 결과물과 함께 “**키**“ 도 같이 전달해야 한다는 것이다.

22. 암호를 만들 때 사용하는 **공개키와 암호를 풀 수 있는 비밀키의 쌍으로 구성된 암호화 방법**을 공개키 혹은 “**비대칭** “ 암호화라고 한다.

23. 비대칭 암호화 방법에서 / 암호를 만들 때 사용하는 “**공개키**” 로는 **암호를 해독할 수 없다**.