DELL Technologies

사이버 보안 치트 시트

갈수록 가상화가 심화되는 환경에서 사이버 범죄가 무서운 속도로 증가하고 있다는 점은 놀라운 일이 아닙니다. 실제로 **사이버 범죄로 인해 2021년에 약 6조 달러의 비용이 발생했습니다**. 이는 미국과 중국에 이어 세계에서 세 번째로 큰 경제 규모입니다.* 공격자들은 날이 갈수록 지능적이고 교묘해지고 있지만 최신 위협을 인지하고 보호 조치를 취하면 온라인 보안을 쉽게 유지할 수 있습니다. **Dell Technologies의 사이버 보안 전문가가 최선을 다해 방지하려는 몇 가지 위협과 직장 및 가정의 보안을 유지하는 방법에 관한 팁을 알려 드리겠습니다.**

드라이브 바이(Drive-by) 침해

팁:
브라우저와 플러그인을 최신 상태로 유지

안전하지 않거나 손상된 웹사이트에 우연히 접속하면 악의적인 공격자가 시스템에 액세스할 수 있습니다.

판별하는 방법:

추가한 적이 없는 시스템의 새 파일 또는 네트워크 연결

구성 정보에 대한 원치 않는 요청

연결이 안전하지 않습니다.

안전하지 않은 하드웨어

팁:
공인 판매자를 통해 구매

프린터가 해킹될 수 있다는 사실을 알고 계셨나요?

위협 행위자는 하드웨어와 액세서리에 취약성을 직접 내장합니다.

판별하는 방법:

지나치게 저렴한 가격의 제품

소셜 엔지니어링

팁:
정부 기관(예: IRS 등)은 먼저 USPS를 통해 연락함

스캐머는 중요한 **개인 또는 금융 정보**를 훔치기 위해 법인 또는 다른 권위 있는 기관으로 가장하여 사람들을 조종합니다(일명 '피싱'). 악성코드는 이메일의 링크나 첨부 파일, 다이렉트 메시지, 문자 메시지를 통해 전송됩니다.

판별하는 방법:

개인 정보를 요청하며 링크 및 첨부 파일을 열도록 지시하는 내용이 포함된 요청하지 않은 이메일 또는 문자

이상한 발신자 이메일 주소, 구문, 철자

여기에 뭔가 수상한 점이 있다고 생각되시나요?

USB 멀웨어 공격

팁:
친구가 공유한 경우라도 알 수 없는 USB 드라이브에 주의

음... 이 USB 드라이브를 연결해도 안전할까요?

범죄자는 USB 드라이브, 휴대용 하드 드라이브, 스마트폰, 음악 플레이어, SD 카드, 옵티컬 미디어(CD, DVD, BluRay)와 같은 이동식 저장 디바이스를 사용하여 컴퓨터나 네트워크를 감염시킵니다.

판별하는 방법:

디바이스의 파일 또는 새로 생성된 파일에 대한 예기치 않은 액세스

신뢰할 수 있는 관계

팁:
강력하고 고유한 비밀번호 사용

해커는 병원과 같이 신뢰할 수 있는 제3자를 침해하고 병원의 평판을 이용하여 환자를 공격합니다.

판별하는 방법:

비정상적인 로그온 동작

본인 인증

사이버 보안을 유지하는 방법:

해야 할 일

모든 계정에 다단계 인증 및 강력하고 고유한 비밀번호를 사용합니다.

인터넷에 연결된 모든 디바이스는 공격에 노출되어 있습니다.
소프트웨어를 최신 상태로 유지하십시오.

경계하고 의심하는 태도를 취합니다. 지속적인 정보를 통해 스캐머의 전략을 인지합니다.

공격에 대해 알립니다. IT 팀에 공격을 보고하고 동료, 가족 및 친구에게 알리십시오.

하지 말아야 할 일

보안과 관련된 조치를 게을리하지 않습니다. 꾸준히 모든 보안 프로토콜을 준수하십시오.

요청하지 않은 이메일이나 다이렉트 메시지에 포함된 링크를 클릭하지 마십시오.

"연결이 안전하지 않습니다" 또는 "연결이 비공개가 아닙니다"와 같은 브라우저 경고를 무시하지 마십시오.

팁:
자세한 정보:
Dell.com/Endpoint-Security

DELL Technologies

---

*Cybersecurity Ventures: 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics