

Introduction to Software Security

Overview of Computer Security (2/2)

Seong-je Cho

Computer Security & Operating Systems Lab, DKU

Sources / References

- Laurie Williams, CSC 515 Software Security, NC State
 - <https://sites.google.com/a/ncsu.edu/csc515-software-security>
- N. Vljajic, EECS 3482: Introduction to Computer Security, Yorku
 - https://www.eecs.yorku.ca/course_archive/2016-17/W/3482/
- Nicholas Weaver, Computer Science 161: Computer Security, Berkeley
- Myrto Arapinis, Computer Security: INFRA10067, University of Edinburgh

- Fran Piessens – KU Leuven, Software Security Knowledge Area, Issue 1.0,
- Software Security, Meenakshi Mani, and Tanvi Shah

Please do not duplicate and distribute

Contents

- **Some famous real world attacks (cont')**
- **What is hackable?**
- **Threats of Stolen Credit Card Numbers**
- **Why is security important?**
- **Who is responsible for Computer Security?**
- **Which skills are required for computer security?**

Some famous real world attacks

(cont')

Personal-information leakage / Privacy breaches

D 청년의사

Published: Oct. 28, 2021

병원 등 12곳 개인정보유출...1억223만 과징금·과태료 처분

개인정보위는 사업자의 유출신고, 경찰 이첩, 이용자의 침해신고를 통해 한국인터넷진흥원(KISA)의 지원을 받아 조사를 진행한 바 있다. 개인정보보호...

Da 디지털데일리

Published: Feb. 23, 2022

해킹된 '상위 1% 소개팅 앱' 14만명 정보 유출... 개인정보위 ...

해킹된 '상위 1% 소개팅 앱' 14만명 정보 유출... 개인정보위 "사생활 침해 심각". 이종현 2022.02.23 15:22:37. 가 +; 가 -. [디지털데일리 이종현기자] '상위 1%

국 국민일보

[단독] 서울대병원, 해킹당했다... 개인정보 유출 가능성도

다만 환자들의 민감한 의료 정보는 이번 해킹으로 유출되지 않은 것으로 파악했다. 국민일보 취재 결과 경찰청 사이버수사대에 최근 서울대병원 해킹 피해...

2021. 7. 8.

M 매일경제

Published: Feb. 23, 2022

개인정보 유출 데이팅앱 '골드스폰' 과징금 1억3000만원

위원회는 "트리플콤마의 안전조치 소홀로 개인정보가 유출되고 해커에 의해 일부 이용자의 개인정보가 공중에 노출되는 등 이용자의 사생활이 현저하게..."

IT IT조선

SK 입사지원자 1600명 개인정보 외부 유출

SK그룹 채용시험 지원자 1600명쯤의 개인정보가 외부에 유출되는 사고가 발생했다. SK측은 재발 방지를 약속했다. SK는 9일 '알려드립니다' 자료를...

2021. 11. 9.

C 조선비즈

'개인정보 유출' 무신사 등 7개 회사에 과태료 4560만원 부과 - 조선비즈

모두 안전조치 의무 위반으로 과징금 부과 대상에는 해당하나 사소한 실수로 개인정보가 유출됐고, 피해 또한 미미했다는 점을 참작했다는 설명이다.

2021. 11. 10.

Personal-information leakage / Privacy breaches

보안뉴스

페이스북 5억명 개인정보 유출... 한국인 12만명도 포함, 사용자 ...

[보안뉴스 권 준 기자] 전 세계 사용자가 22억 명에 달하는 서비스(SNS) 페이스북에서 5억 3,300만명의 개인정보가

2021. 4. 4.

블로터

Published: Feb. 15, 2022

"주민 생체정보 무단수집했다"...메타, 美 텍사스주에 소송 당해

텍사스 주민 수천만명의 생체 정보를 사전 동의 없이 수집해, 사생활을 침해 ... 그러나 해당 기술에 대한 개인정보침해 우려가 지속적으로 제기되자,...



- Facebook (2018) – 2.2 billion
- Yahoo (2013) – 1 billion
- Marriott (2014-18) – 500 million
- Twitter (2018) – 330 million
- Microsoft (2020) – 250 million



- Late 2014, Yahoo announced that data associated with at least 500 million accounts had been stolen.
 - Three months later, it disclosed a second breach affecting more than one billion accounts.
- May 2016, Myspace confirmed a breach of user names and passwords for about 360 million accounts.

The worst data breaches

- Source: These Companies' Data Breaches Impact Their Users the Most, PCMag.com

	Brand	Type of breach	Date	Data collected	Number of people affected
1	Facebook	Hacked	2018		2,200,000,000
2	Yahoo	Hacked	2013		1,000,000,000
3	Facebook	Hacked	2021		533,000,000
4	Yahoo	Hacked	2014		500,000,000
5	Estée Lauder	Data Breach	2020		440,336,852
6	Twitter	Data Breach	2018		330,000,000
7	Microsoft	Data Breach	2020		250,000,000
8	MySpace	Hacked	2016		164,000,000
9	MyFitnessPal	Hacked	2018		150,000,000
10	Ebay	Hacked	2014		145,000,000
11	Decathlon	Data Breach	2020		123,000,000
12	Nametests	Data Breach	2018		120,000,000
13	TK / TJ Maxx	Hacked	2007		94,000,000
14	MyHeritage	Hacked			
15	AOL	Malicious I			


Threat type:
Information disclosure

Data collected key:  All personal details  Credit card information
 Email address and online data  Full bank account details

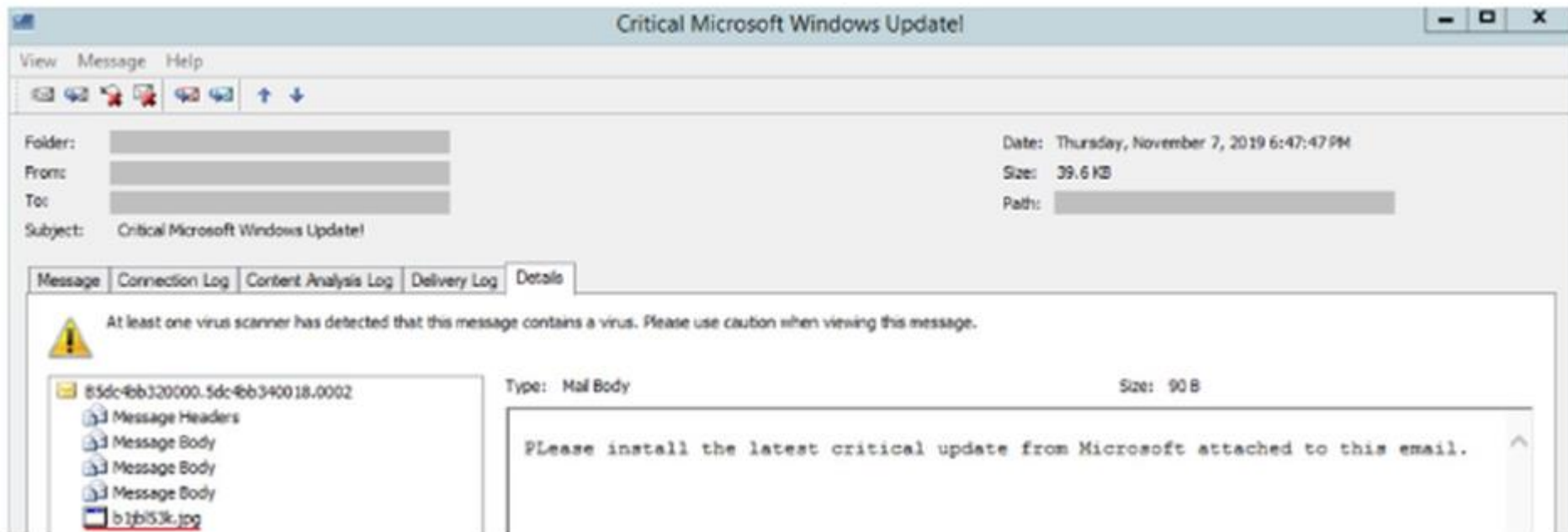
Real World Threats/Attacks

Windows users, beware: This fake update could lock up your PC, or worse

Threat type:
Spoofing,
Fabrication

Alison DeNisco Rayome  November 19, 2019 8:00 AM PST

Updating to Windows 10? Don't fall victim to this spam email attack.




The attachment has a .jpg file extension, but is actually a malicious .NET downloader, which will deliver malware to your machine. The **ransomware**, called **bitcoingenerator.exe**, encrypts the recipient's files, and leaves a ransom note titled "**Cyborg_DECRYPT.txt**" on their desktop, asking for \$500 in bitcoin to unlock the files.

Real World Threats/Attacks

Pacemaker hack can kill via laptop

October 22, 2012 by [InfoSec News](#)

By Jeremy Kirk

 News ▶ World news ▶ FBI

Published: May 17, 2015

FBI probe claims hacker controlled flight through plane's Wi-Fi - and made it fly sideways

IT와 OT의 집합체 '스마트 빌딩', 증가하는 보안위협은 어떻게 대응하나

(2022.03.04 14:08, 보안뉴스)

- IT와 OT, 나아가 Security가 합쳐진 대표적인 스마트 빌딩 '포티넷' 본사 신사옥이 빠르게 변화하면서 빌딩의 의미와 기능이 새롭게 정의되고 있어

우크라 IT군대, 러시아 GPS 겨냥...지구촌은 지금 사이버 전쟁 중

(2022.03.04. 오후 8:29, 이데일리)

- 3일 로이터에 따르면 자발적으로 모인 해커들로 구성된 우크라이나 'IT군대'가 벨로루시 철도 네트워크와 러시아의 자체 위성 항법 시스템 '글로나스' 등을 주요 표적으로 삼고 있어
- 러시아는 이번 전쟁에서 군사 공격에 앞서 '사이버 침공'부터 벌였다. 에너지부, 재무부를 포함한 7개 부처 등의 주요 홈페이지가 러시아가 배후로 의심되는 디도스 공격을 당해

Real World Threats/Attacks

무심코 꽂은 USB, 하루만에 3000억원 날려 (2019.06.26, ChosunBiz)

[Close-up] 초연결사회 보안 비상, 외부 인터넷 접속 막는다고 공격 100% 막을 수 없어

- 2018년 8월 세계 최대 반도체 위탁 생산 기업인 대만 TSMC의 생산라인 3곳이 24시간 가동 중단됐다. 단 하루에 본 피해액만 3000억원 안팎이다. 발단은 오후 9시쯤 한 직원이 생산 설비의 SW를 업그레이드하기 위해 바이러스 검사를 하지 않은 이동식 저장 장치(USB)를 꽂은 것이다. USB에 담겨 있던 악성 바이러스가 공장 생산 설비의 컴퓨터에 침투했다.
- 2010년엔 이란의 핵심 핵(核) 시설이 USB 하나로 뚫리는 해킹 사건이 발생했다. 해커는 외부와 연결되지 않은 폐쇄망을 뚫기 위해 내부 직원들의 USB와 스마트폰을 숙주(宿主)로 삼았다. 이란 핵 시설을 파고든 스텍스넷(Stuxnet) 악성코드는 정교하게 핵심 설비인 원심분리기를 정밀 타격했다.

별명이 '사이버 미사일'이다. 원심분리기를 장시간 동안 빠르게 회전하도록 조종해 결국 고장 나도록 만든다. 심지어 시설 근무자에겐 '정상 가동' 중이라는 표시가 뜨도록 했다.

사이버 공격, 어떤 피해 초래했나

연도	내용	피해규모
2010년	이란 핵시설, 바이러스 감염	원심분리기 1000여 대 마비
2012년	석유 회사 아람코 해킹	컴퓨터 3만5000대 마비. 석유 판매 중단
2014년	한국수력원자력 해킹	원자력발전소 도면 유출
	일본 몬주 원전 악성코드 감염	4만2000개 이상의 작업 기록 등 유출
2015년	우크라이나 전력 시설, 악성코드 감염	6시간 동안 22만여 가구 정전
2016년	미국 한 도메인 업체에 디도스 공격	미국 동부 인터넷 3시간 접속 불가
2017년	일본 혼다, 워너크라이 랜섬웨어 감염	48시간 공장 가동 중단
2018년	대만 TSMC 생산 라인 악성코드 감염	생산 라인 1일간 가동 중단

Real World Threats/Attacks

스턱스넷부터 다크호텔까지 망분리 시스템 공격한 멀웨어 분석했더니 (2021.12.06, 보안뉴스)

- 물리적으로 분리해 놓은 시스템도 사이버 공격자들의 공략 대상이다. 인터넷과 내부 망에서 분리된 컴퓨터를 공격자들은 어떻게 해킹하는 것일까? 이들이 주로 사용하는 17개의 프레임워크를 분석했더니 꽤나 분명한 공통점들이 나왔다.
- 이란의 핵 시설을 무력화했던 Stuxnet 공격 역시 USB의 활용이 있었기에 가능. 망으로부터 분리된 이란 핵 시설의 시스템을 누군가 사이버 공격으로 망가트린 것인데(미국과 이스라엘의 공격으로 여겨지고 있음), 당시 공격자들은 멀웨어가 담긴 USB를 활용. 이 악성 USB는 CVE-2010-2568이라는 취약점을 공략 ...
- 망분리 시스템을 공략하는 많은 공격 프레임워크 등장 -- 한국의 해킹 그룹으로 알려져 있는 DarkHotel이 사용하는 램세이(Ramsay), 중국의 Mustang Panda가 사용하는 플러그엑스(PlugX), NSA와 관련이 있는 공격 단체 Equation Group의 패니(Fanny), 중국의 Goblin Panda가 사용하는 USB컬프리트(USBCulprit) 등이 대표적
- 대부분 윈도 기반 시스템들을 공격하는 데에 초점이 맞춰져 있었으며, 필요한 파일들을 빼돌리는 것에 주력하고 있었다. 75%의 경우 LNK 파일이나 자동실행 파일들이 USB에 삽입되어 있었고, 이 때문에 USB가 시스템에 꽂히는 순간 악성 행위가 시작됐다.
- One-day vulnerabilities (원데이 취약점들)이 주로 익스플로잇 되고 있었다는 것도 공통점이다. “1-day vulnerability이란, 공격이 시작됐을 때 패치가 존재하는 취약점들을 말함. Zero-day는 패치가 없는 취약점. 따라서 망분리 시스템에 대한 패치 관리를 보다 철저히 하는 것 역시 보안에 큰 도움이 됨.”


3줄 요약

1. 유명 망분리 공격 프레임워크 17개 분석했더니 USB라는 공통점 나옴.
2. 다시 말해 USB만 잘 막으면 망분리 시스템 보호가 더 완벽히 된다는 뜻.
3. 공격자들이 USB 통해 원데이 취약점들을 대부분 노린다는 것도 참고해야 함.

Cyber Warfare

Cyberwarfare is the use of digital attacks against an enemy state, causing comparable harm to actual warfare and/or disrupting the vital computer systems.

Countries are using hackers to target power grids, financial markets and government computer systems of rival nations, all with potential results that are every bit as devastating as any bullet or bomb.

 **한겨레** Published: Feb. 24, 2022
러시아, 서방 상대로 '사이버 전쟁' 전개 가능성 : 국제일반 : 국제 ...

작전 본격화하면 민간도 피해 우려. 전쟁 위험이 고조되는 우크라이나에 대한 사이버 공격이 부쩍 늘면서, 러시아가 군사 작전과...

 **The Conversation** Published: March 1, 2022

Intelligence, information warfare, cyber warfare, electronic warfare – what they are and how Russia is using them in Ukraine


Cyber warfare entails infiltrating and disrupting the enemy's computer systems. This includes generating denial of service attacks to block...

 **한국일보** Published: Feb. 16, 2022

우크라 국방부·은행 사이버 공격 당해...러 '하이브리드 전쟁'

...

잇단 공격 배후로 지목된 러시아가 군사적 위협과 동시에 내부 혼란을 부추기고 정보를 빼내는 사이버 공격을 감행하는 '하이브리드 전쟁'을 개시했다는...

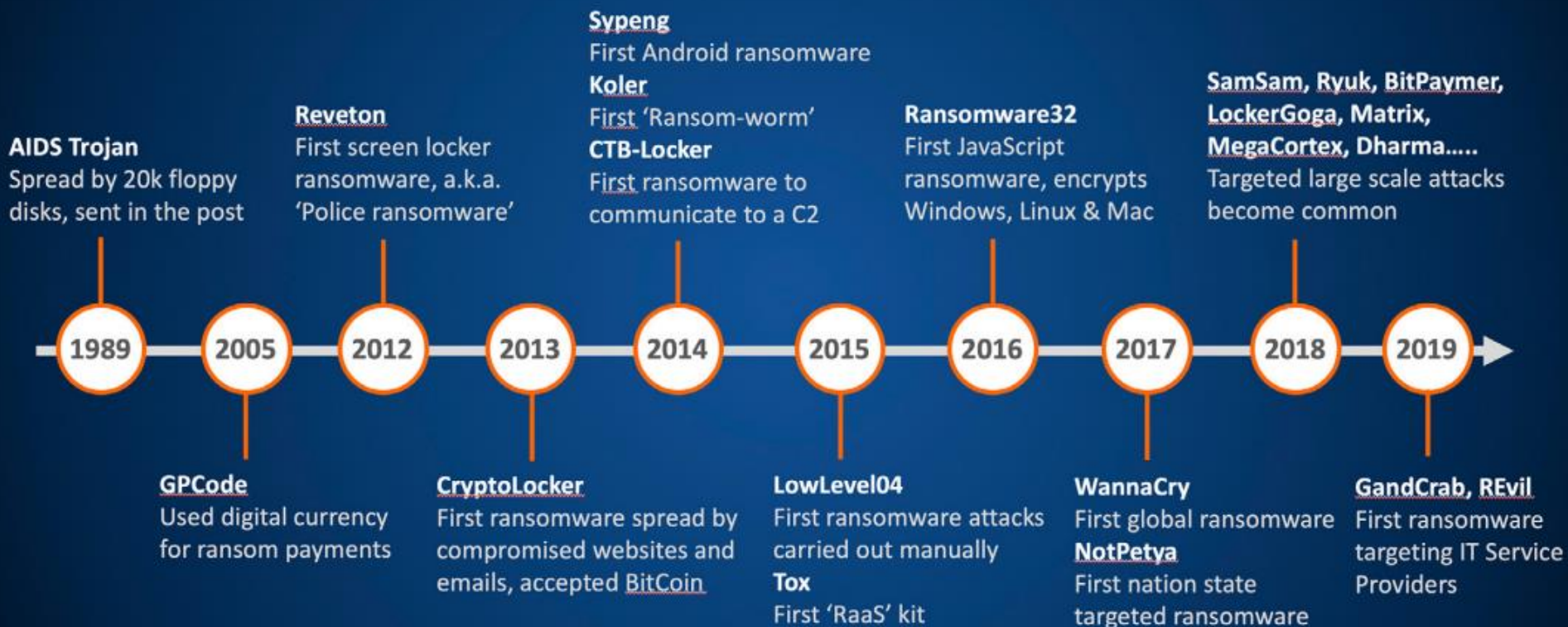
 **블록미디어** Published: March 2, 2022

글로벌 해킹 그룹 어노니머스, 러시아 상대 '사이버 전쟁' 선포

[뉴욕 = 장도선 특파원] 온라인에서 활동하는 해커그룹 어노니머스가 우크라이나를 침공한 러시아를 상대로 사이버 전쟁을 전개하고 있다고 CNBC가 1...

Real World Threats/Attacks

Ransomware Evolved



Real World Threats/Attacks

● 2017 cyberattacks on Ukraine

- A series of powerful cyberattacks using the **Petya malware** began on 27 June 2017 that swamped websites of Ukrainian organizations, including banks, ministries, newspapers and electricity firms.
 - ESET estimated on 28 June 2017 that 80% of all infections were in Ukraine, with Germany second hardest hit with about 9%.
 - Associated Press reported experts agreed that **Petya** was masquerading as ransomware, while it was actually designed to cause maximum damage, with Ukraine being the main target.
 - Petya **encrypts the Master File Table** of the hard drive and forces the computer to restart.
 - It then displays a message to the user, telling them their files are now encrypted and to send US\$300 in bitcoin to one of three wallets to receive instructions to decrypt their computer

- ESET 1992년 설립된 IT 보안 서비스 기업으로, 본사는 슬로바키아 브라티슬라바에 위치해 있음.
- Associate Press (AP): 미국연합통신은 미국 뉴욕에 위치한 다국적 비영리 통신사로, 미국에서 가장 오래된 유서 깊은 최대의 통신사다

Real World Threats/Attacks

● 2017 cyberattacks on Ukraine

- Security experts found that the version of **Petya** used in the Ukraine cyberattacks had been modified, and subsequently has been named **NotPetya** or **Nyetna** to distinguish it from the original malware.
 - **NotPetya** encrypted all of the files on the infected computers, not just the Master File Table, and in some cases **the computer's files were completely wiped** or rewritten in a manner that could not be undone through decryption.
 - Some security experts saw that the software could intercept passwords and perform administrator-level actions that could further ruin computer files.
- NotPetya는 일종의 사이버 무기
- NotPetya는 MEDoc (세무회계 SW)의 업데이트 기능을 통해 감염되어 확산됨.

2017 Cyberattacks on Ukraine

- Attackers compromised the update channel for MeDoc
 - MeDoc is Ukrainian S/W company's package (M.e.Doc는 회계 SW 패키지)
 - An analyst (Nichols) discovered an alarming vulnerability in the update servers for MeDoc
 - An update for MeDoc was pushed out by the update server, following which the ransomware attack began to appear
- They then monitored for weeks with their **backdoor**
- Then they released a malicious "**worm**"
 - A program which self-propagates: spreads from computer to computer in an institution
 - And then disabled all the infected computers with a fake "ransomware" payload
 - This cost Maersk shipping alone **\$100M-300M** in lost revenue!
 - » A.P. Moller-Maersk (뮐러-머스크사—해운회사. 덴마크의 복합 기업) is the world's largest container shipping company
 - Maersk may lose up to \$300M due to **NotPetya** attack

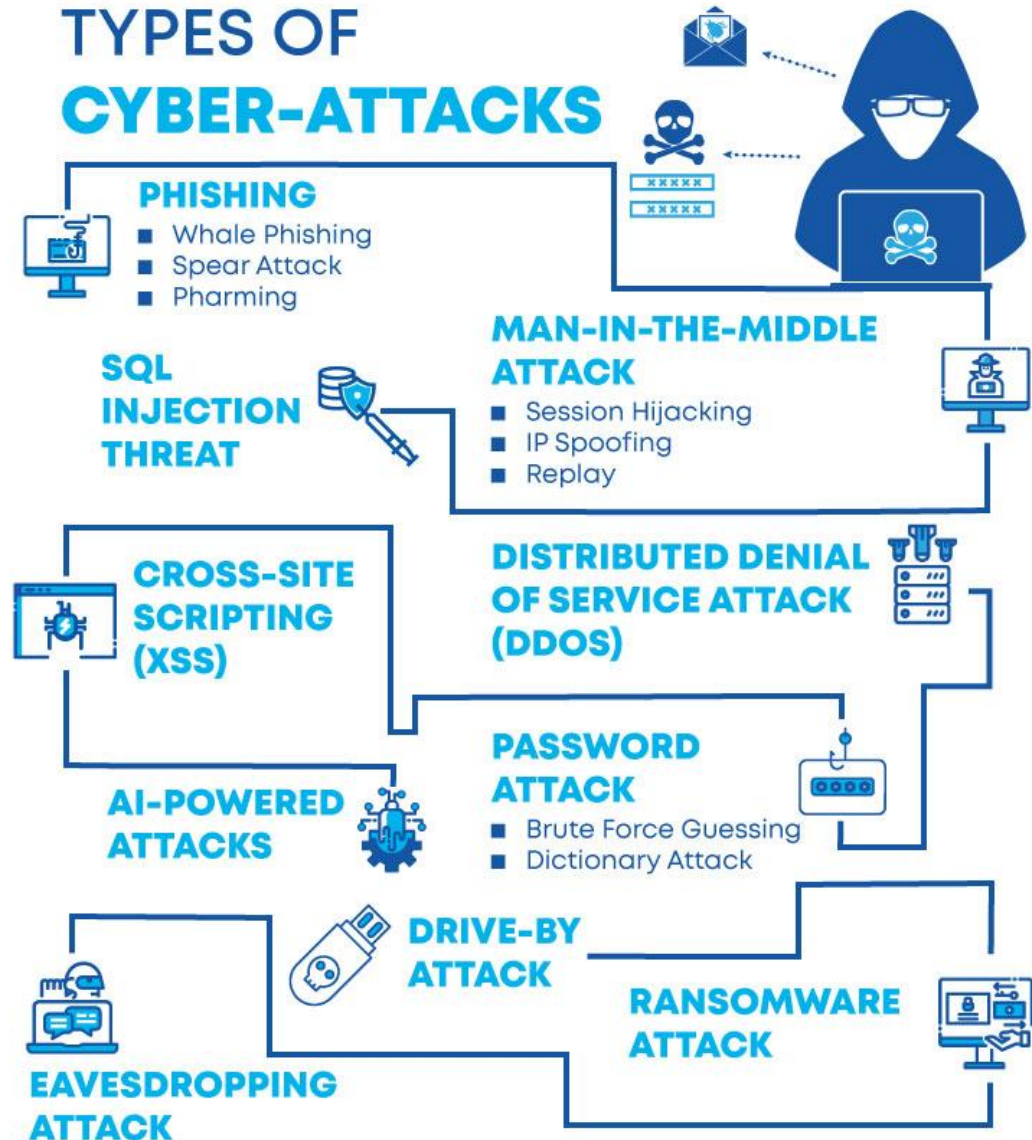
Types of Cybersecurity attacks

Phishing

- A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.
- 개인정보(Private data) + 낚시(Fishing)
- Such criminals use disguise, pretending to be someone their victims can trust.
- Then they trick them into opening a message, email, or link.

Pharming

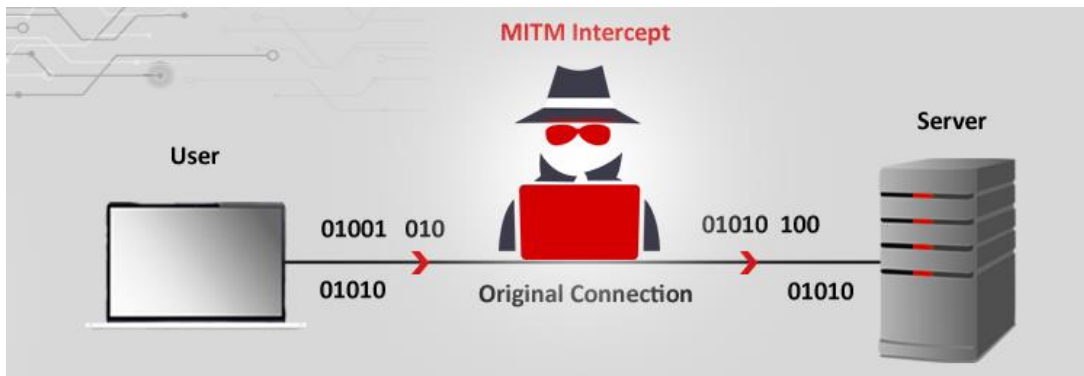
- Using technical means to redirect users into accessing a fake Web site masquerading as a legitimate one and divulging personal information.
- Pharming is a fraudulent act that directs users to a fake page that looks like the original, to steal from them



Types of Cybersecurity attacks

● Man-in-the-middle attack (MitM)

- An attack in which an attacker is positioned between two communicating parties in order to intercept and/or alter data traveling between them.
 - In the context of authentication, the attacker would be positioned between claimant and verifier, between registrant and CSP (Credential Service Provider) during enrollment, or between subscriber and CSP during authenticator binding.
- A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.
- 중간자 공격은 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격 기법



Source: Prashant, Cyber Attacks Explained – Man In The Middle Attack

Types of Cybersecurity attacks

- Drive by download attacks

- **two types, each concerning the unintended download of computer software from the Internet,**
 - **Authorized Drive-by downloads** are downloads which a person has authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet).
 - **Unauthorized Drive-by downloads** are downloads which happen without a person's knowledge, often a computer virus, spyware, malware, or crimeware.
- They specifically refer to malicious programs that install to your devices — without your consent.
 - 웹 사이트를 방문하거나 이메일 메시지를 볼 때 또는 유혹하는 팝업 윈도우를 클릭할 때 발생 가능
- A drive-by download attack refers to the unintentional download of malicious code to your computer or mobile device that leaves you open to a cyberattack.
- You don't have to click on anything, press download, or open a malicious email attachment to become infected.
- A drive-by download can take advantage of an app, OS, or web browser that contains security flaws due to unsuccessful updates or lack of updates.

Types of Cyber Security Threats to College Students



Source: <https://medium.com/@aryacollege/types-of-cyber-security-threats-to-college-students-11c449a108a3>

Types of Cyber Security Threats to College Students

- **Malvertising** (malware advertising)

- an attack in which perpetrators inject malicious code into legitimate online advertising networks. The code typically redirects users to malicious websites. (defined by imperva.com)
- It is the use of online advertising to spread malware.
 - It typically involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.
- Internet advertising whose real intention is to deliver malware to the viewer's computer.



Your PC is infected!

Scan now

[Update your antivirus \(free\)](#)

- **Rogue security software**

- a form of malware and internet fraud that misleads users into believing there is a virus on their computer and aims to convince them to pay for a fake malware removal tool that actually installs malware on their computer.
- **Rogue antivirus**: 백신 소프트웨어를 사칭해서 이득을 얻는 악성 소프트웨어. 주로 설치된 컴퓨터에 악성코드가 감염되었다는 등의 거짓 내용을 띄워 사용자를 속여 결제 유도

Source: [Wikipedia](#)

Threats from the Dark Web

다크웹 통한 불법 거래 규모 지속해서 늘고 있어

출처: [특집] 나날이 커지는 사이버 위협 '2022 사이버 보안 트렌드' 전망,
CEONews, 2021.12.14

2022년에는 '다크웹(Dark Web)'을 통한 정보 거래 및 유통이 더 활발히 이뤄질 것으로 예상된다. '다크 웹'은 암호화된 네트워크에 기반을 두고 있어 일반적인 검색 엔진이나 브라우저를 통한 접근이 제한된다. 초기에는 해커들의 기술 공유 목적으로 사용되었지만, 몇 년 전부터는 강력한 익명성을 토대로 마약, 총기 등은 물론 개인 정보 및 기업 주요 정보 등을 거래하는 사이버 범죄의 온상으로 자리 잡게 되었다.

실제로 다크웹 상의 불법 거래 규모는 지속적인 증가 추이를 보인다. 한국인터넷진흥원(KISA)에 따르면, 2019년 기준 국내 다크웹 접속자 수는 하루 평균 15,000명에 달했다. 이는 2016년과 비교해 3배 이상 늘어난 수치이다.

다크웹 시장은 특유의 익명성을 토대로 불법 행위와 관련된 거래의 장 역할을 하며 빠르게 확대될 것으로 보인다. 다크웹을 통한 기업 기밀 정보 및 개인 정보 판매 문제는 꾸준히 제기되고 있으나, 기업 인프라에 접근 가능한 원격 접속 계정 등이 무분별하게 거래되고 있어 현재로서는 그 피해 규모를 산정하기조차 어려운 상황이다.

또 다크웹에서는 불법적인 정보 거래와 더불어 '워터링홀(watering holes)', '웹 스키머(web skimmers)', '분산 서비스 거부(DDoS)', 랜섬웨어 등을 서비스 형태로 제공하는 '청부 해킹' 거래도 이뤄지고 있어, 더욱 강력한 대응 전략 마련이 요구된다.

[2022 보안 핫키워드-1] 다크웹의 대중화 추세, 사이버범죄의 확산을 이끌다, 보안뉴스, 2021-12-21

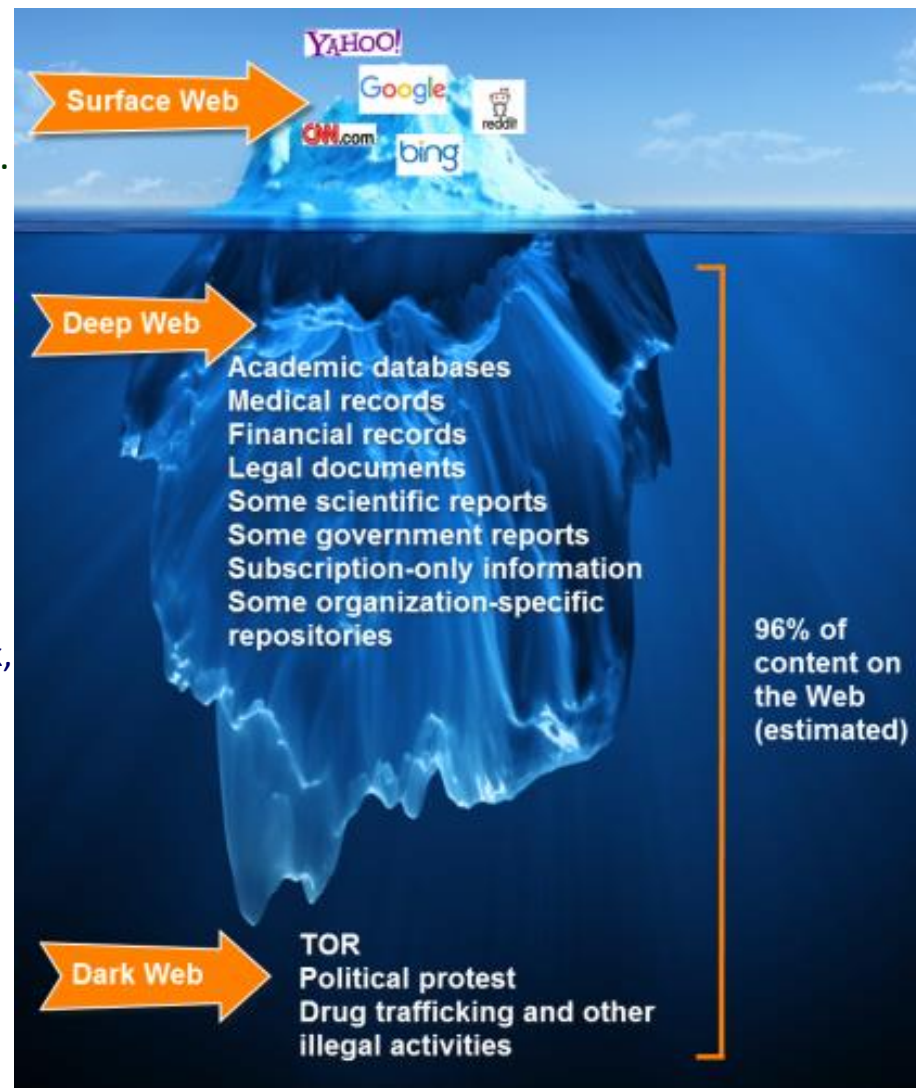
Dark Web & Deep Web

Deep Web

- parts of the World Wide Web whose contents are not indexed by standard web search-engines.
 - content behind memberships, and internal company or government data not for public consumption.

Dark Web

- A collection of thousands of websites which are not indexed by conventional search engines.
 - They often use anonymity tools, like the Tor network, to hide their IP address and preserve the anonymity of the creators and visitors.
- The World Wide Web content that exists on darknets: overlay networks that use the Internet but require specific software, configurations, or authorization to access



Source: Net Neutrality: Why It Matters, Sutori

What is hackable?

Threats of Stolen Credit Card Numbers

What is hackable?

- Everything!
- Especially things connected to the Internet

Why Hackers Are Trying to Get Into Your Refrigerator

It's not to steal your peanut butter. The ever-growing Internet of Things has turned home appliances and other consumer devices into potential gateways for far-reaching cyberattacks.



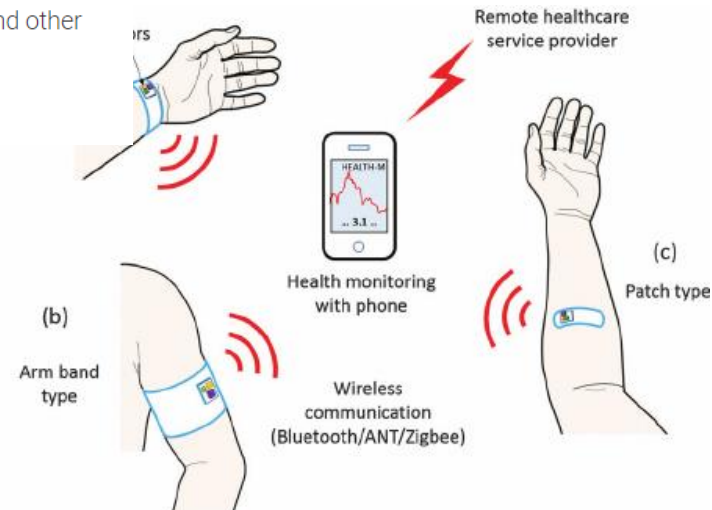
By Will Yakowicz Staff writer, Inc. [@WillYakowicz](#)

For The First Time, Hackers Have Used A Refrigerator To Attack Businesses



Julie Bort

Business Insider January 17, 2014



Source: https://www.researchgate.net/figure/Three-types-of-wearable-sensor-nodes-powered-by-thermoelectric-energy-harvesters-The_fig1_279634036

Palo Alto: More than 100,000 infusion pumps vulnerable to 2 vulnerabilities Published by ZDNet, Mar. 8, 2022

In an examination of more than 200,000 infusion pumps on the networks of several healthcare organizations, Palo Alto Networks security researchers discovered that more than 52% were susceptible to two known vulnerabilities that were disclosed in 2019 – one with a "critical" severity score and the other with a "high" severity score.

What is hackable?

Couple says smart home system was hacked: 'It gives me the chills'



By Daniella Genovese, FOXBusiness

Asset image of the Google Nest Learning Thermostat – 3rd Generation. (Google Nest)

A Milwaukee couple was left feeling “violated” after their home camera began talking to them, their thermostat suspiciously topped 90 degrees and vulgar music blasted through their wireless electronics.

What is hackable?

What you should know about hackable home security systems, [CTV News Vancouver, Feb. 23, 2022](#)

- Jamming is when a burglar or hacker blocks the wireless signal of a door sensor, window sensor or motion sensor in a security system. That allows them to access your home without actually triggering the alarm.
- In its latest tests, Consumer Reports found five home security systems susceptible to these types of attacks: Adobe Iota, Cove Home Security, Eufy 5-Piece Home Alarm Kit, Ring Alarm, and SimpliSafe the Essentials. Abode and SimpliSafe can detect jamming and will alert the homeowner that happens, but the alarms won't trigger. The other systems offer no user alerts.



Samsung Hacked: Millions Of Devices Could Be Exposed, [Channelnews, 6 Mar 2022](#).

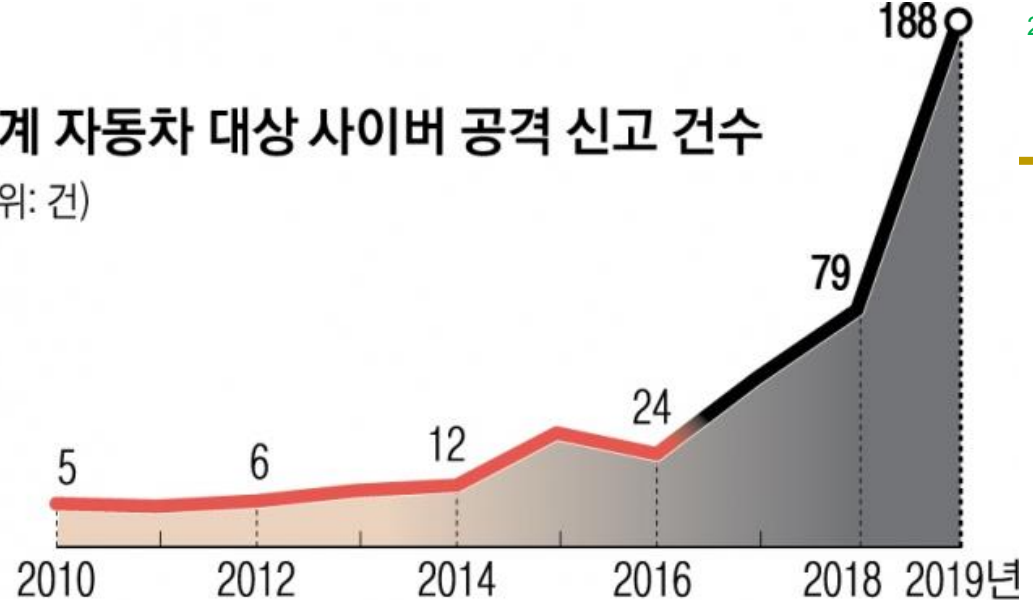
- Samsung Electronics has been hacked by a foreign hacking group, believed to be South American, who claim that they have the authentication code behind **Samsung's Knox security system** and the biometric log in codes which could give them access to millions of **Samsung smartphones tablets** and **PC's** including tens of thousands sold Australia.

What is hackable?

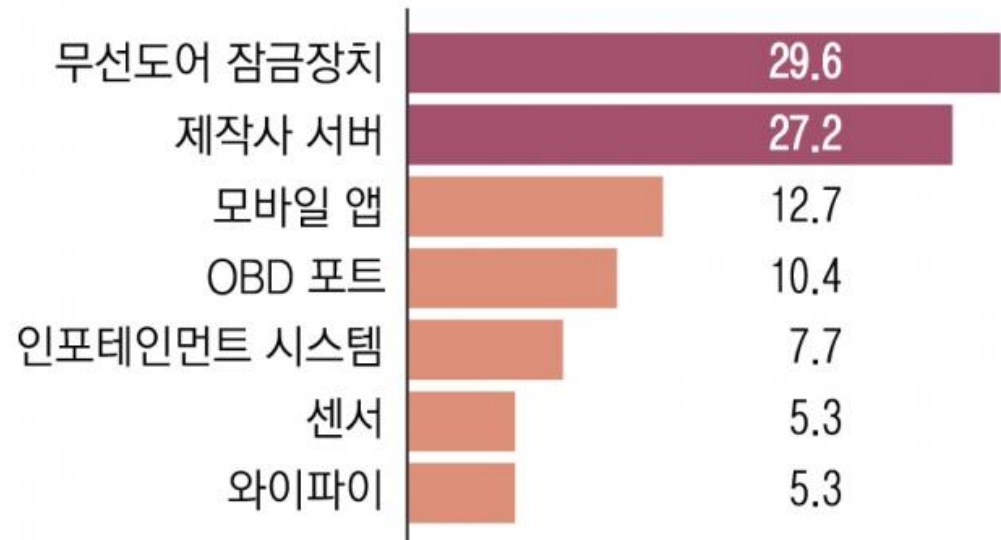
- 해킹당한 순간 통제불능...
스마트카, 도로 위 폭탄 우려
(2020.09.21 서울신문)

- <6>똑똑해진 車, 사이버 공격엔 무방비
- 2018년 9월 미국 텍사스주 와코에서 21세 청년이 자동차 절도 혐의로 경찰에 체포됐다. 이 청년은 렌터카 업체로부터 전기차인 테슬라 '모델S'를 훔쳐 도주하다 사흘 만에 붙잡혔다. 용의자는 테슬라의 스마트폰 애플리케이션을 해킹해 자동차 문을 열고, 위성항법시스템(GPS)을 무력화시켜 이동경로 추적을 피했던 것으로 드러났다.

세계 자동차 대상 사이버 공격 신고 건수
(단위: 건)



자동차 사이버 공격 주요 경로 (단위: %)



※전체 사고 건수에서 각 경로 비율을 산출한 것으로 중복 가능

〈자료: 한국교통안전공단, 업스트림시큐리티〉

자동차 사이버보안 위협

● 자동차까지 보안을 걱정해야 하네요.

자동차를 대상으로 한 사이버범죄는 나날이 증가해 사회적 문제로 확대하고 있습니다. 2010년부터 2021년까지 발생한 자동차 관련 사이버 보안 범죄를 분석한 결과, 자동차 해킹으로 인한 주요 피해는 데이터 범죄 및 사생활 침해(39.9%), 자동차 절도 및 탈취(27.9%), 자동차 조종 시스템 해킹(24.2%), 서비스/비즈니스 방해(19.2%), 사기(4.2%), 자동차 시스템 조작(4%), 위치 추적(2%), 정책 위반(1.5%) 순으로 나타났습니다.

- 특히, 대부분의 범죄는 지난 2년간 발생. 기술이 발전할수록 더 많은 범죄가 발생할 것으로 예측.

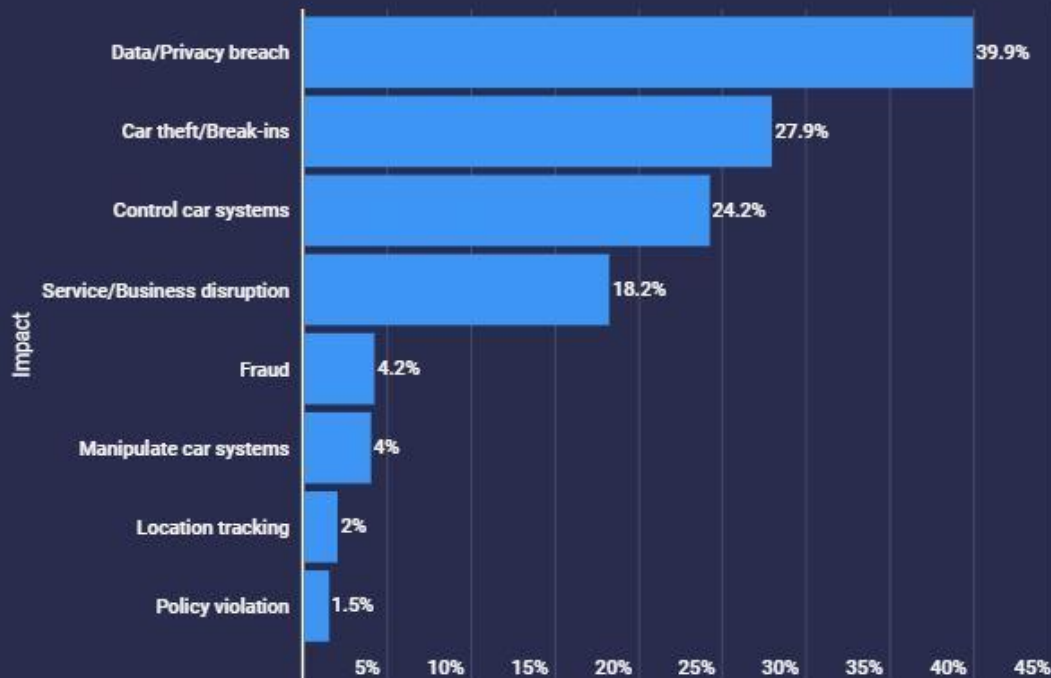
출처: [모빌리티 인사이트] 당신의 차는 안전한가요? 자동차용 사이버 보안, 동아일보, 2022-03-03 기사,

출처 (우측 그림): 지난 10년 간 자동차 해킹으로 인한 주요 피해, AtlasVPN



Impact breakdown of 900+ automotive-related cyber incidents (2010-2021)

FACT: more than 50% of all reported automotive-related cybersecurity incidents took place during the past two years alone.



Source: Upstream Auto Ltd.

How Do Credit Card Numbers Get Stolen?

Spyware
Keylogger

Drive-by download

Contactless Scenario 1:

● methods of 'operation' by Hacking

- malware installed on a **corporate server**
- malware installed on a **public computer** – malware skims credit card details whenever user logs in their bank number, credit card number, email address, password ...
- malware installed on a **public server** – malware downloaded to a client machine at every visit of infected Web-site

Contactless Scenario 2:

● methods of 'operation' by Phishing

- malware sent via email as attachment / link
 - user must be fooled at opening attachment / link and initiating malware installation
- phishing = most common 'attack vector' in most (corporate) hacks

👉 Phishing -- a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a person into revealing sensitive information to the attacker or to deploy malware on the victim's infrastructure like ransomware.

Where Do Stolen Credit Card Numbers Go ?

- **Credit Card Brokers**

- Black market 'agents' who buy and re-sell stolen credit card numbers

Number	Type	Name	Country	City	Phone	Mail	DOB	Price	Select
372845	AMEX	Charles J. B.	US	LA 90075	Y	N	Y	40\$	<input type="checkbox"/>
528713	MasterCard	Christopher B.	US	Chicago IL 60604	Y	N	Y	40\$	<input type="checkbox"/>
645450	DISCOVER	David Webb	US	NY 10018	Y	N	Y	40\$	<input type="checkbox"/>
371527	AMEX	J. Bowers	US	LA 90008	Y	N	Y	40\$	<input type="checkbox"/>
646880	DISCOVER	John Smith	US	Louisville KY 40203	Y	N	Y	40\$	<input type="checkbox"/>
651920	DISCOVER	John J.	US	NY 10075	Y	N	Y	40\$	<input type="checkbox"/>
645857	DISCOVER	J. Bowers	US	NY 10018	Y	N	Y	40\$	<input type="checkbox"/>
371198	AMEX	J. Bowers	US	Chicago IL 60604	Y	N	Y	40\$	<input type="checkbox"/>


What is the selling price for stolen credit card numbers?

http://www.theregister.co.uk/2013/07/02/mcafee_cybercrime_exposed/

Crimelords: Stolen credit cards... keep 'em. It's all about banking logins now

Also, Crimeware-As-A-Service is a thing. Really

By John Leyden 2 Jul 2013 at 08:24

39  SHARE ▼

Stolen bank login information attracts an even higher price than credit card numbers on underground cybercrime bazaars, and EU logins are worth more than American ones, according to research by McAfee

Dumps	Estimate of Prices (without PIN, with PIN, PIN and good balance)									
	US			EU			CA, AU		Asia	
Visa Classic	\$15	\$80		\$40	\$150		\$25	\$150	\$50	\$150
Master Card Standard	\$90			\$140			\$150		\$140	
Visa Gold/Premier	\$25	\$100	\$200	\$45	\$160	\$250	\$30	\$160	\$55	\$150
Visa Platinum	\$30	\$110		\$50	\$170		\$35	\$170	\$60	\$170
Business/Corporate	\$40	\$130		\$60	\$170		\$45	\$175	\$70	\$170
Purchasing/Signature	\$50	\$120		\$70			\$55		\$80	
Infinite				\$130	\$190		\$60	\$200		\$190
Master Card World	\$140									
AMEX	\$40			\$60			\$45		\$70	
AMEX Gold	\$70			\$90			\$75		\$100	
AMEX Platinum	\$50									

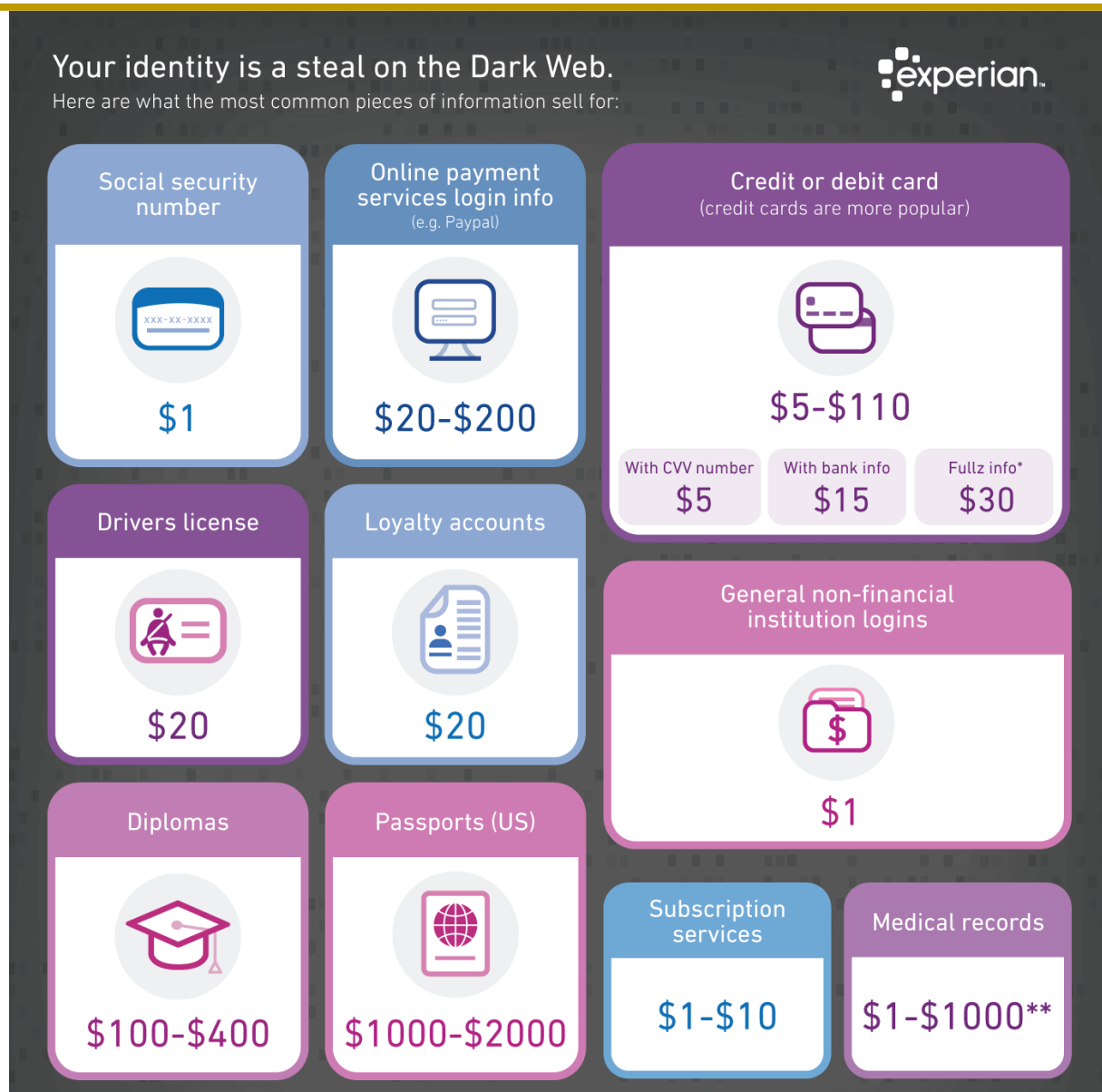
Here's How Much Your Personal Information Is Selling for on the Dark Web - 33 -

- Posted by Brian Stack on Dec. 2017

<https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

What Information Is Most Common and How Much Is It Worth?

- Fulz** (=full information) is a bundle of info that includes a “full” package for fraudsters: name, SSN, birth data, account numbers, and other data
- Value of Medical records depends on how complete they are as well as if it is a single record or an entire DB



Why is security important?

**Who is responsible for
computer security?**

Why is security important?

- **Computer Security allows the University to carry out its mission by:**
 - Enabling people to carry out their jobs, education, and research
 - Supporting critical business processes
 - Protection personal and sensitive information

- **It is important for our**
 - Physical safety
 - Confidentiality / Privacy
 - Functionality
 - Protecting our assets
 - Successful business
 - A country's economy and safety
 - and so on ...

디지털 전환 시대에서의 사이버 보안

- **자동차 보안, 선택 아닌 '필수'** (공학저널: 2020.08.28)
자율주행, 커넥티드카 보안의 핵심은 소프트웨어를 넘어 하드웨어까지 자동차 전체를 아우르는 보안 기술로 확장되고 있다
- **도시 치안에서 환자 생명까지..."글로벌이 주목하는 IoT 보안"** (조선일보: 2020.02.04)
- **MS, 코로나19 이후 보안 위협 多...클라우드 보안 중요** (HelloT 산업경제: 2020.08.27)
- **내년 '블록체인·메타버스·마이데이터' 보안 허점 공격 증가 전망** (ZDNet코리아: 2021.12.23) – 메타버스 환경에서의 불법 행위 기승
- **"미래보안분야는 AI의 각축장"** – 해커 AI 통해 침입탐지시스템 공격...기업도 AI 서비스 확대 (아이뉴스24: 2020.09.18)
- **코로나19가 유망직업도 바꿨다...전 세계 뜨는 일자리는?** (동아일보: 2020-09-20)
미국의 경우 지난 1일 미 노동부가 발표한 2019~2029 고용전망 보고서만 보더라도 앞으로 10년간 증가율이 높은 10개 직업 중에 8개가 헬스케어와 IT 산업 관련 직종이 꼽혔다. 전문 임상간호사(NP), 작업치료 보조사, 재택·개인 건강보조원, 물리치료 보조사, 의료서비스 매니저, 의사보조자(PA), **정보보안 분석가**, 통계학자 등이다.

자율 자동차 보안

구분	설명	보안위협 유형
전장 플랫폼	<ul style="list-style-type: none"> ▲ 임베디드 시스템의 자원제약으로 인한 ECU의 보안설계 미흡으로 발생하는 접근제어 무력화 ▲ 인증·권한획득 우회, 펌웨어 위·변조 등의 공격 	<ul style="list-style-type: none"> △ ECU SW결함 △ ECU 리버스 엔지니어링 △ ECU 펌웨어 해킹 및 위·변조 △ 위장 ECU 장착 △IVI(In-Vehicle Infotainment)해킹 △ 스마트 센서 물리공격(블라인드, Spoofing, Jamming)
내·외부 네트워크	<ul style="list-style-type: none"> ▲ 내·외부 통신 도청, 패킷 위·변조, 리플레이, 스푸핑 등 공격 ▲ 저가형 네트워크 프로토콜로 인한 오류처리 매커니즘 취약 	<ul style="list-style-type: none"> △ 정상 네트워크 방해(패킷삽입, 삭제, 임의조작, 지연) △ 무선 통신망 해킹, △ 악의적 차량(Misbehavior Vehicle) △ 거짓정보(Fake Message) 제공 △ 차량접속기기 해킹
관리 및 진단	<ul style="list-style-type: none"> ▲ 보안취약점 및 테스트를 위한 표준화 기술 부재로 잠재적 위협 내재화 ▲ 사후 분석 위주의 증거분석 문제 	<ul style="list-style-type: none"> △ 프라이버시 침해 △ 원격 업데이트 및 진단 프로토콜 해킹 △ 사고 발생시 증거보존의 한계

출처: 한국전자통신연구원 '자율주행 자동차 보안기술 동향', 내용 일부 재구성

구분	설명	보안위협 대응 방안
전장 플랫폼	<ul style="list-style-type: none"> ▲ 임베디드 시스템 가상화 및 오토사(AUTOSAR, AUTomotive Open System ARchitecture) 보안기능을 활용한 ECU 보안성 강화 	<ul style="list-style-type: none"> △ 시큐어부트, 시큐어플래시, 접근제어 △ 애플리케이션 샌드박스, 플랫폼 가상화 △ HSM(Hardware Security Module) △ 부채널 방지 △ 오토사 CSM (Cryptographic Security Manager), SecOC(Security Onboard Communication)
내·외부 네트워크	<ul style="list-style-type: none"> ▲ 국제표준(IEEE 1609.2)을 준용한 DSRC, 웨이브(WAVE) 기반 통신보안 ▲ CAN 중심의 통신보안기술을 기반으로 CAN-FD, 이더넷(Ethernet)에 대한 보안기술로 확대 	<ul style="list-style-type: none"> △ FW, IDS, IPS △ ECU 인증, 키관리, 암호화 △ 위협탐지(Rule Based, Machine Learning Based) △ V2X 메시지 인증, 암호화 △ 차량PKI, V2X 메시지 서명(고속) 검증 △IEEE 1609.2, CAMP VSC3
관리 및 진단	<ul style="list-style-type: none"> ▲ 장비나 네트워크 연결지점에 대한 모의해킹 진단이 주로 수행 ▲ 사고원인 분석은 기술 개발 진행 	<ul style="list-style-type: none"> △ 보안 모니터링, 보안취약성 분석 △ 차량 이상징후, 비정상 행위 분석 △ 원격 SW/FW 보안 업데이트 △ J2735 기반 보안성 평가 △ 포렌식 및 사고 원인 분석 기술

출처: 한국전자통신연구원 '자율주행 자동차 보안기술 동향', 내용 일부 재구성

출처: [기고] 자율주행차 기술 요소 및 보안 위협 대응전략, IT Daily, 2021.06.30

Who is responsible for computer security?

“In the last 20 years, **technology has permeated every facet of the business environment.**

- The business place is no longer static –it moves whenever employees travel from office to office, from office to home, from city to city.
- Since business have become more fluid, ..., **computer security is no longer the sole responsibility of a small dedicated group of professionals, ..., it is now the responsibility of every employee”**
- The Internet can be a hazardous place.
- A compromised computer is a hazard to everyone else, too – not just to you
- **Question:** What can a hacked computer be used for/to?

Permeate: 침투하다, 스며들다. Facet: 측면, 양상

General Security & Privacy Tips for College Students

- Regularly Check Your Bank Statements
- Back Up Your Data Frequently
- Think Before You Click -- Never click on anything that may be suspicious.
- Use Public Computers Wisely
 - there are times public computers come in handy, like those in campus libraries. Be sure that you do not accidentally save any passwords, and always log out of all accounts before walking away.
- Shop on Secure Websites Only
- Ensure that Security Systems are Up-to-Date
- Be Careful Who You Provide Personal Information To
- Prepare for a Potential Data Breach (if it happens, be ready to change all passwords)

Source: The College Student's Guide to Data Protection & Cybersecurity, by Security.org Team, Jan. 16, 2019

- **Protect your cyber threats on college campuses**
 - Using a VPN, confirming the network name, disabling the automatic connect function to make them verify the network authentic before connecting.
 - Campus Wi-Fi is not much more secure than any public Wi-Fi
 - Avoid leaving valuables, and Installing laptop tracking software
 - Avoid putting sensitive information or visiting any sites that seem suspicious

Good Security Standards follow the “90 / 10” Rule:

- *10% of security safeguards are technical*
- *90% of security safeguards rely on the **computer user** (“YOU”) to adhere to good computing practices*

Example: *The lock on the door is the 10%.*

You remembering to lock the lock, checking to see if the door is closed, ensuring others do not prop the door open, keeping control of the keys, etc. is the 90%.

You need both parts for effective security.

What Does This Mean for Me?

- This means that everyone who uses a computer or mobile device needs to understand how to keep their computer, devices and data secure.
 - *Computer Security is **everyone’s** responsibility*

Everyday Security & Privacy

Some key steps for Security that everyone should

- Use **good, cryptic passwords** that can't be easily guessed - and keep your passwords secret
- Make sure your computer, devices and apps are current and **up to date**
- Make sure your computer is protected with up-to-date **anti-virus and anti-spyware SW**
- **Don't click** on unknown or unsolicited links or attachments, and **don't download** unknown files or programs onto your computer or other devices
- Remember that information and passwords sent via standard, unencrypted wireless are especially easy for hackers to intercept
 - *To help reduce the risk, look for “https” in the URL before you enter any sensitive information or a password*
 - *Also avoid standard, unencrypted email and unencrypted Instant Messaging (IM) if you're concerned about privacy*

“Everyday security”

● “Everyday security”

- Password managers
- Password changing strategies
- Two-Factor Authentication (2FA)



Source:

<https://surepassid.com/products/multi-factor-authentication-mfa/>

- OTP tokens - how do they work? Why are they better?
- IoT - for the devices you carry around; smart home; smart cities
 - Firmware update
- Alexa; Cortana; Siri
 - Cortana: a virtual assistant created by Microsoft for Windows 10, Windows 10 Mobile, Windows Phone 8.1, Invoke smart speaker, Microsoft Band, Surface Headphones, Xbox One, iOS, Android, Windows Mixed Reality, and Amazon Alexa.

■ . . .

피싱 예방

- Phishing is a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person..
- **개인정보(Public data) + 낚시(Fishing)**
 - 금융 정보나 개인 식별 정보 등의 개인정보를 낚아 이를 악용하는 사기 수법입니다.
- 대표적인 방식은 금융기관을 가장한 이메일을 발송해 금융정보를 탈취하는 것입니다.
 - 이용자가 금융기관에서 발송된 이메일이라 믿고, 안내된 인터넷 주소를 클릭하면 가짜 은행 사이트로 접속됩니다.
 - 그리고 시키는 대로 보안카드 번호 등 금융 정보를 입력하면 그대로 정보가 탈취되고, 금전 피해를 입는 것입니다.
- **피싱, 이렇게 예방하세요!**
 1. 이메일, 문자메시지에서 출처가 불분명한 링크나 첨부파일은 함부로 클릭하지 않습니다.
 2. 보안카드 전체의 번호를 입력해야 하는 일은 없습니다.
 3. 접속하려는 사이트 주소의 정상 여부를 확인합니다. 문자열 순서나 특수문자를 사용해 교묘하게 다르지 않은지 확인합니다.

출처: [카드뉴스] 왕초보 용어 풀이, 피싱이란? 보안뉴스 (2017-12-04)

14 Personal Data Security Tips For Everyday Users

Source: Forbes Technology Council, May 11, 2020

1. Back up your data
2. Enable Multi-Factor Or Two-Step Authentication
3. Check The Email Address Domain
4. Use A Password Manager
5. Hover Over URLs Before Clicking To Ensure Legitimacy
6. Read The EULA (End User License Agreement)
 - You can understand “Who owns the data, how will it be used and where will it be stored?”
7. Always Use a VPN
8. Disable Location Services And Microphone Access Where Not Needed
9. Don't Ignore Software And OS Updates
10. Invest In an OCR (optical character recognition) Scanner for securing documents (PDFs)
11. Set Up Face ID and Fingerprint Features
12. Never Reuse Passwords
13. Subscribe To Haveibeenpwned.com
 - haveibeenpwned.com can identify if your login info has been part of a data hack or breach.
14. Use Long, Memorable Passphrases
 - On Wi-Fi, keep things up-to-date (just like your computer!) and put a passphrase on that too. Something like "My-WiFi-is-not-free-for-the-whole-neighborhood" works great!

Top Compute Security Skills in High Demand

The Top Skills Required for Cybersecurity Jobs

- **Problem-Solving Skills**
- **Technical Aptitude**
 - cybersecurity is a technology-focused field: you will be likely be tasked with responsibilities such as troubleshooting, maintaining, and updating information security systems; implementing continuous network monitoring; and providing real-time security solutions.
- **Knowledge of Security Across Various Platforms**
- **Attention to Detail**
 - You are required to be highly vigilant and detail-oriented, in order to effectively detect vulnerabilities and risks.
- **Communication Skills**
- **Fundamental Computer Forensics Skills**
- **A Desire to Learn**
- **An Understanding of Hacking**

Source: <https://online.champlain.edu/blog/top-cybersecurity-skills-in-high-demand>

Summary, Q & A

- Some famous real world attacks
 - Big Data Breaches
 - Cyber warfare, Phishing

- Everything is hackable.
 - Things connected to the Internet
 - Connected & autonomous vehicles, Connected medical devices
 - IoT, IoMT, ...

- Keep your Credit Card Number secret.

- Everyone is responsible for computer security.

- Top Security Skills in high demand

Conferences & Exhibitions

- **CodeGate** - <http://codegate.org/>
 - International Hacking Competition Online (해킹방어대회)

- **SECON** - <https://www.seconexpo.com/>
 - International Security Exhibition & Conference

- **POC Conference**
 - <http://powerofcommunity.net/>

- **Black Hat**
 - Asia, USA, Europe
 - <https://www.blackhat.com/>

- **Best of The Best (BoB)**
 - Next-generation Security Leader Training Program
 - <https://www.kitribob.kr/>

Appendix

What will you try to learn in this class?

- How to *think adversarially* about computer systems
- How to *assess threats* for their significance
- How to build programs & systems with *robust security properties*
 - If I find out you start a new project in C or C++, or use unescaped SQL, or allow your web site to support CSRF attacks...
 - **MY SPIRIT WILL REACH THROUGH YOUR MONITOR AND STRANGLE YOU!!!!**
- How to gauge the protections and limitations provided by today's technology
- How attacks work *in practice*
 - Code injection, logic errors, browser & web server vulnerabilities,

The biggest data breaches

● Source: Quartz, CSO from IDG

			Company	Accounts Hacked	Date of Hack
2018	Marriott	500m	Yahoo	3 billion	Aug. 2013
2017	Equifax	143m	Marriott	500 million	2014-2018
2016	Adult Friend Finder	412.2m	Yahoo	500 million	Late 2014
2015	Anthem	78.8m	Adult FriendFinder	412 million	Oct. 2016
2014	eBay	145m	MySpace	360 million	May 2016
	JP Morgan Chase	76m	Under Armor	150 million	Feb. 2018
	Home Depot	56m	Equifax	145.5 million	July 2017
Biggest Data Breaches of the 21 st century					
2013	Yahoo		EBay	145 million	May 2014
	Target Stores	110m	Target	110 million	Nov. 2013
	Adobe	38m	Heartland Payment Systems	100+ million	May 2008
2012	US Office of Personnel Management (OPM)	22m	LinkedIn	100 million	June 2012
2011	Sony's PlayStation Network	77m	Rambler.ru	98 million	Feb. 2012
	RSA Security	40m	TJX	94 million	2003-2004
2008	Heartland Payment Systems	134m	AOL	92 million	2004
2006	TJX Companies, Inc.	94m	MyHeritage	92 million	Oct. 2017

SOURCE: CSO

Real World Threats/Attacks

● Can affect a country's economy

Kim Zetter / Wired:

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

— It was 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their workday and head home through the cold winter streets. Inside the Prykarpattiaoblenergo control center ...



The hackers who struck the power centers in Ukraine—the first confirmed hack to take down a power grid—weren't opportunists who just happened upon the networks and launched an attack to test their abilities. (03.03.16)

Inside the Prykarpattiaoblenergo control center, which distributes power to the region's residents, operators too were nearing the end of their shift. But just as one worker was organizing papers at his desk that day, the cursor on his computer suddenly skittered across the screen of its own accord.

He watched as it navigated purposefully toward buttons controlling the circuit breakers at a substation in the region and then clicked on a box to open the breakers and take the substation offline. A dialogue window popped up on screen asking to confirm the action, and the operator stared dumbfounded as the cursor glided to the box and clicked to affirm. Somewhere in a region outside the city he knew that thousands of residents had just lost their lights and heaters.

The operator grabbed his mouse and tried desperately to seize control of the cursor, but it was unresponsive. ...

BlackEnergy malware activity spiked in runup to Ukraine power grid takedown

But its role in the attack remains unclear

By John Leyden 4 Mar 2016 at 20:47

10 SHARE ▼

Importance of Good Passwords

● The Real Lessons Of Gawker's Security Mess – Forbes, Dec. 2010

The first thing the Gnosis group does in the synopsis it released of their attack is identify Nick Denton's (founder of Gawker Media) password, and point out that it is the same password he uses for Gawker's Google Apps account and on his twitter account @nicknoted.

They go on to provide 16 more Gawker staffer's e-mail addresses, user names, and passwords.

The passwords, 15 of which are strings that are either common dictionary words or slight variations thereof and one that is the person's name and 1, indicate that Gawker has no password composition policy (how long passwords should be, that they should contain letters/numbers/special characters) for employees.

They also determined his password on the campfire team collaboration tool instance used by Gawker (a real time chat utility) and with it extracted 4 gigabytes of Gawker chat logs.

From within those chat logs the attackers were able to extract FTP servers, usernames, and credentials for the sites thq.com, valvesoftware, rockstargames, lucasarts, scea, kotaku, and 2kgames.

<https://www.forbes.com/sites/firewall/2010/12/13/the-lessons-of-gawkers-security-mess/#6abce5126b5d>