Software Ethics

We have the opportunity to build products that change the world in positive ways. Don't be like these guys:

> Two alleged owners of Mugshots.com ... have been arrested ... The notorious website publishes mugshots and then demands payment for their removal... "This pay-for-removal scheme attempts to profit off of someone else's humiliation," said Attorney General Becerra in a statement. "Those who can't afford to pay into this scheme to have their information removed pay the price when they look for a job, housing, or try to build relationships with others. This is exploitation, plain and simple." - Ars Technica on May 18, 2018

> **Ashley Madison Used Chatbots to Lure Cheaters, Then Threatened to Expose Them When They Complained** - It turns out a company established to facilitate unethical behavior made some ethical lapses of its own. In a statement last week, Ashley Madison parent company Avid Life Media confirmed long-circulating suspicions that it used "bots" to give users the impression that the site had more female users than it actually did... Meanwhile, CNN Money reports that customers who disputed charges from the site were told that records of their activity would be mailed to their home, essentially a threat to expose them to spouses and families - Fortune on July 10, 2016

Even so, sometimes our creations can be used in unintended and unfortunate ways:

> Facebook told congressional investigators on Wednesday that it sold political ads during the 2016 U.S. presidential election to a so-called Russian troll farm that was looking to target American voters... Facebook sells its advertising through a self-service ad model, through which buyers can choose demographic, geographic and interest-based targets... Due to the volume of these ad buys, Facebook said it was unable to identify the inauthentic nature of these ad buys at the time. - CNN on September 7, 2017

> San Francisco-based company reached an agreement with California's housing agency amid complaints of guests being rejected for their race... On social media, black Airbnb users reported experiences of facing a rejection by a host, who later accepted them when they changed their profile to a white person. Earlier this month, an Asian American woman's account of discrimination in California went viral after she said a host cancelled on her last minute specifically because of her race, leaving her stranded in a storm. ... Harvard Business School professor Ben Edelman previously found that black users were 16% less likely to be accepted than identical guests with white names... - The Guardian on April 27, 2017

> More than two weeks ago, hackers seized parts of the computer systems that run Baltimore's government. It could take months of work to get the disrupted technology back online. That, or the city could give in to the hackers' ransom demands. "Right now, I say no," Mayor Bernard Young told local reporters on Monday. "But in order to move the city forward? I might think about it. But I have not made a decision yet." ... A copy of a digital ransom note, obtained by The Baltimore Sun, stated that the city could unlock the seized files for a price: three Bitcoins (nearly $24,000) per system or 13 Bitcoins (about $102,000) for them all. - The New York Times on May 22, 2019

Malware

The term **Malware** refers to software that is created with malicious intent.

> Malware is an abbreviated term meaning "malicious software." This is software that is specifically designed to gain access or damage a computer without the knowledge of the owner. There are various types of malware including spyware, keyloggers, true viruses, worms, or any type of malicious code that infiltrates a computer.
>
> Generally, software is considered malware based on the intent of the creator rather than its actual features. Malware creation is on the rise due to the sheer volume of new types created daily and the lure of money that can be made through organized Internet crime. Malware was originally created as experiments and pranks, but eventually led to vandalism and destruction of targeted machines. Today, much of malware is created for profit through forced advertising (adware), stealing sensitive information (spyware), spreading email spam or child pornography (zombie computers), or to extort money (ransomware). - Norton website

> Malware is any software or mobile application specifically designed to harm a computer, a mobile device, the software it's running, or its users. Malware exhibits malicious behavior that can include installing software without user consent and installing harmful software such as viruses. - Google website

Specific categories of malware include:

- **Virus** - "designed to spread from host to host and has the ability to replicate itself" (source)
- **Adware** - while not strictly "malicious", adware is used to serve advertisements to users
- **Spyware** - detects computing activity without the user's knowledge
- **Phishing** - "uses fraudulent emails or texts, or copycat websites to get you to share valuable personal information – such as account numbers, Social Security numbers, or your login IDs and passwords", which are then used to "steal your money or your identity or both" - (source)
- **Ransomware** - cripples computer systems and demands a ransom in return for restoring the systems to normal operations

Recent malware attacks in the news:

> Arizona Beverages, one of the largest beverage suppliers in the U.S., is recovering after a massive ransomware attack last month, TechCrunch has learned.
>
> The company, famous for its iced tea beverages, is still rebuilding its network almost two weeks after the attack hit, wiping hundreds of Windows computers and servers and effectively shutting down sales operations for days until incident response was called in, according to a person familiar with the matter.
>
> More than 200 servers and networked computers displayed the same message: "Your network was hacked and encrypted." The company's name was in the ransom note, indicating a targeted attack... The ransom note asked to email the attacker "to get the ransom amount." - TechCrunch on April 2, 2019

> Last Friday, the City of Atlanta was struck by a ransomware attack that took much of the city's internal and external services offline. As of today, many of those services have been restored, but two public portals remain offline. On Saturday, the automated dispatch network for Baltimore's 911 system was also taken offline by an apparent ransomware attack. And yesterday, Boeing's Charleston facility—which manufactures

> components for Boeing's 777 and other commercial jets, and for the Air Force's KC-46 tanker—was struck by what was initially reported to be WannaCry malware. - Ars Technica on March 29, 2018

> The hackers' weapon of choice on Friday was Wanna Decryptor, a new variant of the WannaCry ransomware, which encrypts victims' data, locks them out of their systems and demands ransoms. - New York Times on June 27, 2017

> A vulnerability first uncovered by the National Security Agency and then released by hackers on the internet is now being used in one of the most prolific cyberattacks ever around the globe. It's called WannaCry, and it's brought computer systems from Russia to China to the UK and the US to their knees, locking people out of their data and demanding they pay a ransom or lose everything. So far, more than 200,000 computers in 150 countries have been affected, with victims including hospitals, banks, telecommunications companies and warehouses. - CNet on May 19th, 2017.

Hacking

Black-hat vs **White-hat** Hacking:

> White hats are security researchers or hackers who, when they discover a vulnerability in software, notify the vendor so that the hole can be patched.
>
> Black hats are criminals. They use their prowess to find or develop software holes and attack methods (aka zero day vulnerabilities and exploits) or other malicious tools to break into machines and steal data, such as passwords, email, intellectual property, credit card numbers or bank account credentials. They also sell information about the security holes to other criminals for them to use. - Wired