1. **Mark your confusion.**
2. **Show evidence of a close reading.**
3. **Write a 1+ page reflection.**

You Have Almost Certainly Been Hacked

Source: TheWeek.com, October 15, 2017

Hackers are breaking into the systems of companies, government agencies, and individuals. Is any information safe? Here's everything you need to know:

How many people have been hacked?

So much information has been stolen by hackers that virtually everyone in the U.S. has been affected by a data breach in some way — even those who never go online. The recent data breach at Equifax, one of the three major credit reporting agencies, exposed the personal information of more than 145 million Americans, including Social Security numbers, driver's license data, birth dates, and addresses. As many as 75 percent of U.S. adults with a credit score may have been victimized. While the Equifax attack was particularly damaging, it was hardly unique. Hackers exposed the personal information of 110 million people in 2013 and 2014, nearly half the nation's adults. In those years, more than 40 million credit and debit card numbers were stolen in a single attack against Target. Yahoo had all 3 billion of its accounts hacked. "It's a safe assumption that everyone's Social Security number has been compromised and their identity data has been stolen," said Jeremiah Grossman, the chief of security strategy at the cybersecurity firm SentinelOne. "While it may not be explicitly true, we have to operate under that assumption now."

Are the breaches getting worse?

Yes. Almost 2 billion records were lost or stolen worldwide during the first half of this year, up 164 percent from the last half of 2016. IBM has found that the average cost of a single data breach is now $7.35 million in the U.S. The Equifax hack has already cost the company $4 billion in market value. Spending on cybersecurity is soaring as a result, and is expected to reach $90 billion this year and $113 billion by 2020, according to consulting firm Gartner. In 2015, a report by the Atlantic Council think tank and Zurich Insurance Group concluded that while the benefits of online technology will lead to an 8 percent increase in the size of the global economy between 2010 and 2030, the cost of security will start to outweigh the benefits around 2019.

Why is data so vulnerable?

Poor security practices are partly to blame. Despite the overall rise in spending on cybersecurity, many companies neglect to keep their systems regularly updated and patched. Equifax blamed a single employee for not installing a software update that would have prevented the breach. Many organizations and government agencies are reluctant to upgrade because of the cost and service disruption involved, leaving so-called legacy technology in place for years. About 7 percent of computers around the world still run 2001's Windows XP, making it the third most popular operating system. But Microsoft stopped supporting XP in 2014, leaving it highly vulnerable to hackers. Most data is also stored unencrypted. Only 4 percent of breaches since 2013 have been so-called secure breaches, in which the data involved is encrypted, rendering it useless to those who steal it.

Who's responsible?

The list of offenders includes state-sponsored hackers, criminal gangs, and "hacktivist" groups, with the lines often blurring between them. The Chinese have recruited a "hacker army" estimated at between 50,000 and 100,000 strong, including special military units, that is dedicated in part to seizing valuable data from U.S. companies and government agencies. The Russian military has focused heavily on recruiting hackers wherever it can find them, including from university programs, software companies, and even the criminal underworld. To maintain plausible deniability, the Russian government sponsors hacker collectives such as "Fancy Bear" and "Cozy Bear," which pulled off successful spear-phishing attacks against the Democratic National Committee in 2016. Experts say that the Equifax hack appears similar to recent state-sponsored attacks on the insurance company Anthem and the U.S. Office of Personnel Management, with the hackers using tools favored by Chinese intelligence. But it's also getting easier for non-state actors to pull off major attacks. Sophisticated hacking tools can be bought on the dark web for as little as $100. "It's increasingly easy for anybody to wield the kind of capability that used to be reserved for nation-states, or required nation-state level of expertise and investment," says Nate Fick, CEO of cybersecurity firm Endgame.

Is any defense possible?

Technologists are working furiously on new strategies. One idea is to use artificial intelligence to monitor networks for suspicious activity that would otherwise go unnoticed, acting as a digital "immune system." Some researchers are developing hardware that's built for security from the ground up, including computer chips that can't be fooled by bogus instructions. But even under ideal conditions, the nature of computing makes attacks inevitable. It's estimated that programmers commit about 50 errors per every 1,000 lines of code. The latest version of Windows is roughly 50 million lines long, and the Android smartphone operating system has 12 million lines of code. Even after rigorous checking, bugs get through. Then there's the potential for human error: Hillary Clinton's campaign chairman, John Podesta, made the 2016 Russian hack possible by clicking on a spear-phishing link, giving hackers access to his emails. "The attackers only have to find one weakness," says Kathleen Fisher, a computer scientist at Tufts University. "The defenders have to plug every single hole, including ones they don't know about."

Hacking the hackers

With hackers becoming more brazen, some in the security community are advocating that businesses go on the offensive, breaking into their attackers' systems to steal back or delete stolen data or even damage their computers. Earlier this year, Rep. Tom Graves (R-Ga.) proposed a bill, known as the Active Cyber Defense Certainty Act, that would exempt companies victimized by cyberattacks from laws that prohibit them from accessing others' systems without permission. The strategy is controversial. Many hackers commandeer other people's computers and servers to launch attacks, making it likely that counterattacks could hit innocent systems, creating more chaos in an already chaotic cybersecurity landscape. But hacking back is already being practiced quietly by many businesses, said Davi Ottenheimer, president of security consultancy FlyingPenguin. "Almost every large organization I consult with has some form of hack-back going on," he said.

Possible Response Questions:

- What are your thoughts about computer hacking? Explain.
- What steps do you take to protect your personal information? Explain.
- Discuss a “move” made by the writer in this piece that you think is good/interesting. Explain.
- Pick a passage from the article and respond to it.