THE WALL STREET JOURNAL.

https://www.wsj.com/articles/see-how-much-you-really-know-about-cybersecurity-11559672037

JOURNAL REPORTS: TECHNOLOGY

See How Much You Really Know About Cybersecurity

Take this Wall Street Journal quiz, with questions on the hackability of biometrics, whether you should pay ransom to hackers, and more

By Catherine Stupp
June 4, 2019 2:13 pm ET

Companies spend huge amounts of time and money teaching employees how to guard against cyberattacks. And for good reason: Cyberattacks have the ability to disrupt business operations, damage technology and harm corporate reputations.

JOURNAL REPORT

- Read more at WSJ.com/journalreporttech

MORE IN CYBERSECURITY

- The Quantum Threat to Encryption
- Our Emotional Attachment to Our Passwords
- Can the Sound of Your Typing Be Decoded?
- The Tussle Over Facial Recognition

But building an adequate defense isn't easy, as hackers always seem to be one step ahead of corporate efforts to stop them.

So, how much do *you* know about cybersecurity? Take our quiz and find out.

1. How much did the White House last year estimate that malicious cyber activity cost the U.S. economy in 2016?

A. As much as $14 billion

B. As much as $37 billion

C. As much as $109 billion

D. As much as $1 trillion

Answer C. The White House Council of Economic Advisers in its early 2018 report also said that insufficient sharing of information by companies regarding "common cyber vulnerabilities" is hurting cybersecurity efforts.

2. Which of the following companies have reported a large data breach in the past year?

A. Marriott International Inc.

B. British Airways

C. Adidas AG

D. Humana Inc.

E. All of the above

Answer: E. No industry is immune to hackers. These firms experienced a variety of cyberattacks, including one that collected data from the British Airways website as customers booked flights. At Humana , a network server was hacked. Marriott said intruders were likely lurking in its Starwood Hotels guest systems for two years before Marriott acquired the company in 2016, and for another two years after that.

3. What is the most common way data is breached?

A. Ransomware

B. Phishing

C. Corrupting mobile phones

D. Intercepting data on public Wi-Fi

E. Using hacking tools leaked from the National Security Agency

Answer: B, according to a report by Verizon Communications Inc. Hackers disguise phishing emails to look legitimate but the emails contain malicious links to trick employees or consumers into revealing their credentials. Many people are fooled.

4. How much are companies and governments expected to spend on cybersecurity products and services this year globally?

A. $50 million

B. $50 billion

C. $124 million

D. $124 billion

E. $224 billion

Answer: D. This is a jump of more than 8% compared with last year, according to the report from Gartner Inc. citing the figures. The additional spending is being spurred in part by increasing regulatory requirements and the shortage of cybersecurity professionals.

5. How much does cyber crime cost the global economy?

A. $1 trillion

B. $350 billion

C. $600 billion

D. $175 billion

Answer: C. Cyber crime costs the world an estimated $600 billion, or 0.8% of global GDP, according to a 2018 report from McAfee and the Center for Strategic and International Studies.

6. Biometric data such as facial scans or fingerprints can't be hacked.

A. True B. False

Answer: False. Cybersecurity researchers have shown that voice recordings and fingerprints can be edited to trick detection software.

7. Should you pay the ransom demanded by hackers who lock up your device or data?

A. Yes

B. No

C. It depends

Answer: No. The U.S. government doesn't encourage cyber crime victims to pay ransom to hackers. Victims should consider that criminals may not restore their data even if they pay.

8. Do most Americans view cyberattacks from other countries as a major threat to the U.S.?

A. Yes

B. No

C. The number is evenly split.

Answer: Yes. Seventy-four percent of Americans see cyberattacks from other countries as a top threat to the U.S., according to a 2019 survey from the Pew Research Center. When asked to choose what they saw as a top threat to the U.S. from among a list of potential threats, more Americans chose cyberattacks than Islamic State, climate change, North Korea's nuclear program, Russia, China, or the condition of the global economy.

9. Where were the biggest financial losses in the U.S. from cyber crimes in 2018?

A. Washington, D.C.

B. New York

C. Texas

D. California

E. Massachusetts

Answer: D. Victims from California reported total losses of more than $450 million to the Federal Bureau of Investigation's Internet Crime Complaint Center last year. New Yorkers experienced the second-highest level of losses, at around $201 million.

10. What is the average salary for a woman of color in cybersecurity?

A. $75,000

B. $85,000

C. $95,000

D. $105,000

E. $115,000

Answer: E. This is 7% less than the average salary of $124,000 for a white male in the field, according to research from Frost & Sullivan, ISC(2) and the Center for Cyber Safety and Education. Men of color and white women each earn $121,000 on average.

11.Under the European Union's General Data Protection Regulation, how soon after discovering a data breach are companies required to report the incident to regulators?

A. 30 days

B. 7 days

C. 24 hours

D. 72 hours

E. Notification is only recommended in the event of a malicious cyberattack.

Answer: D. The GDPR requires any company that does business in the EU to notify regulators

about breaches that expose personal data within 72 hours after discovering them. If companies fail to comply, they can face fines of as much as 4% of global revenue or €20 million ($22 million), whichever is larger.

12.What percentage of companies in the energy, health-care and manufacturing sectors experienced damaging cyberattacks in the past two years?

A. 50%

B. 20%

C. 78%

D. 90%

E. 15%

Answer: D. Ninety percent of businesses in these sectors suffered a cyberattack that led to data breaches, significant disruption or downtime of business operations, according to a 2019 survey from cybersecurity firm Tenable Inc. Sixty-two percent of companies in these sectors experienced two or more damaging cyberattacks in the past two years.

13. What country did the U.S. government say was responsible for the November 2014 cyberattack on Sony Pictures?

A. Russia

B. China

C. North Korea

D. Iran

E. The U.S. never publicly blamed a foreign country for the hack.

Answer: C. The FBI said in December 2014 that the North Korean government was behind the Sony attack. In September 2018, the U.S. Justice Department announced charges against one North Korean individual for his role in the attack.

Ms. Stupp is a reporter for The Wall Street Journal in New York. She can be reached at catherine.stupp@wsj.com. Kim Nash, deputy editor of WSJ Pro Cybersecurity, also contributed to this quiz. She can be reached at kim.nash@wsj.com.

Appeared in the June 5, 2019, print edition as 'Quiz See How Much You Know About Cybersecurity.'

- College Rankings
- College Rankings Highlights
- Energy
- Funds/ETFs
- Health Care
- Leadership
- Retirement
- Small Business
- Technology
- Wealth Management