ShinyHunters claim FBI medical data leak

LEVEL B1


Photo: Unsplash

I. WARM-UP

1. What personal data do you protect most carefully?
2. How can you spot a phishing message?
3. What should victims do after a cyber attack?

II. KEY VOCABULARY

vulnerable
at risk of being hurt, harmed or tricked

blackmail
getting something by threatening to reveal private information

impersonate
to pretend to be another person

breach
a break in security that lets attackers in

phishing
sending fake emails or messages to steal data or passwords

retraction
an official statement taking back earlier advice or words

extortion
using threats or pressure to force someone to do something

dataset
a large, organised collection of related data

III. READING

Cyber-criminal group ShinyHunters says it stole sensitive medical records for thousands of FBI special agents. Samples seen by reporters include blood and urine test results and doctors' notes about allergies.

Experts warn the breach could leave agents vulnerable to scams, blackmail and phishing, and help criminals impersonate officers. The hackers issued an extortion demand. It is not for money but for a retraction of a May FBI advisory. They say they will publish the full dataset in five days unless the FBI agrees.

The FBI has acknowledged the breach and says it is investigating how it happened. ShinyHunters claims it exploited a vulnerability in an Oracle cloud system used by the FBI. The group says this let it reach platforms such as FBIJobs, FBI BEAST, MedLink and BICS.

It now claims to hold data on about 60,000 current and former staff, including some senior officials, though this is not confirmed.

Reading text adapted from reporting by **BBC News***: "Special agents' blood and urine test results...". Original article linked at theenglishwire.com.*

IV. COMPREHENSION QUESTIONS

1. Who does ShinyHunters say it stole data from?
2. What medical details were in the sample records?
3. What did the hackers demand instead of money?
4. When do they say they will publish the data?
5. Which FBI systems did the group say it accessed?

V. DISCUSSION

1. Should police and security staff get extra data protection? Why?
2. Is it ever right to negotiate with hackers? Why or why not?
3. What steps should organisations take after a major breach?
4. How could leaked medical data affect someone's life?

VI. GRAMMAR FOCUS

Future continuous

Use will be + verb-ing to describe actions that will be in progress at a specific time in the future.

"Investigators **will be checking** *evidence tomorrow."*
"An agent **will be preparing** *a statement next week."*

VII. GRAMMAR EXERCISE

Complete each sentence with the future continuous form of the verb in brackets.

1. At this time tomorrow investigators (review) ___ logs. _____
2. Tomorrow afternoon security teams (monitor) ___ platforms. _____
3. This time next week, reporters (follow) ___ the story closely. _____
4. Next week analysts (investigate) ___ how it happened. _____
5. By this time next month experts (study) ___ the breach. _____

Teacher's Notes

TEACHERS ONLY

These notes are designed to help you get the most out of this lesson. Please do not share this page with students.


Photo: Unsplash

I. LESSON GUIDE

- Timing: 8–10 minutes warm-up, 10 minutes vocabulary, 12–15 minutes reading and comprehension, 8–10 minutes grammar, 10–12 minutes discussion.
- Pre-teach key terms (vulnerable, breach, phishing, retraction, extortion) with quick examples, then check students can pronounce ShinyHunters and the FBI system names.
- Run a two-stage reading: first skim for who/what/when; then scan for details like what was stolen and the hackers' demand. The topic involves crime and personal safety, so let students comment on the news rather than their own data if they prefer.
- Differentiate: stronger students write a 3–4 sentence risk summary; others fill a table (who/what/how/so what) before discussing.

II. DISCUSSION FACILITATION TIPS

1. Start with a show of hands, then ask pairs to list two benefits and two risks.
2. Set up mini-debates in pairs; after 3 minutes, swap sides and argue the opposite.
3. Elicit a 4-step checklist on the board, then compare with partners' ideas.
4. Prompt concrete examples: jobs, insurance, family, travel; ask for short stories.

III. EXTENSION ACTIVITIES

Writing: Write a 70-word internal notice the FBI could send to staff after the breach.

Debate: In groups, plan and deliver 1-minute arguments for or against meeting the hackers' demand.

IV. ANSWER KEY OVERVIEW

Comprehension questions: short factual answers from the text.

Grammar exercise: Future continuous

Discussion: open-ended. Accept any reasonable ideas supported by examples and reasoning.

Answer Key

TEACHERS ONLY

These answers are for teachers only. Please do not share this page with students.


Photo: Unsplash

IV. COMPREHENSION QUESTIONS

1. Who does ShinyHunters say it stole data from?
   FBI special agents and staff.
2. What medical details were in the sample records?
   Blood and urine test results and doctors' notes about allergies.
3. What did the hackers demand instead of money?
   A retraction of a May FBI advisory.
4. When do they say they will publish the data?
   In five days, unless the FBI agrees.
5. Which FBI systems did the group say it accessed?
   FBIJobs, FBI BEAST, MedLink and BICS.

V. DISCUSSION

Open answers. Accept any reasonable ideas supported by examples and reasoning.

VII. GRAMMAR EXERCISE

Complete each sentence with the future continuous form of the verb in brackets.

1. At this time tomorrow investigators ___ logs. **will be reviewing**
2. Tomorrow afternoon security teams ___ platforms. **will be monitoring**
3. This time next week, reporters ___ the story closely. **will be following**
4. Next week analysts ___ how it happened. **will be investigating**
5. By this time next month experts ___ the breach. **will be studying**

VI. GRAMMAR FOCUS

Key point: Use will be + verb-ing to describe actions that will be in progress at a specific time in the future. (Examples constructed.)

"Investigators **will be checking** *evidence tomorrow."*
"An agent **will be preparing** *a statement next week."*