

Tietoevry ransomware attack causes outages for Swedish firms, cities

By

[Lawrence Abrams](#)

- January 21, 2024
- 03:13 PM
- [0](#)

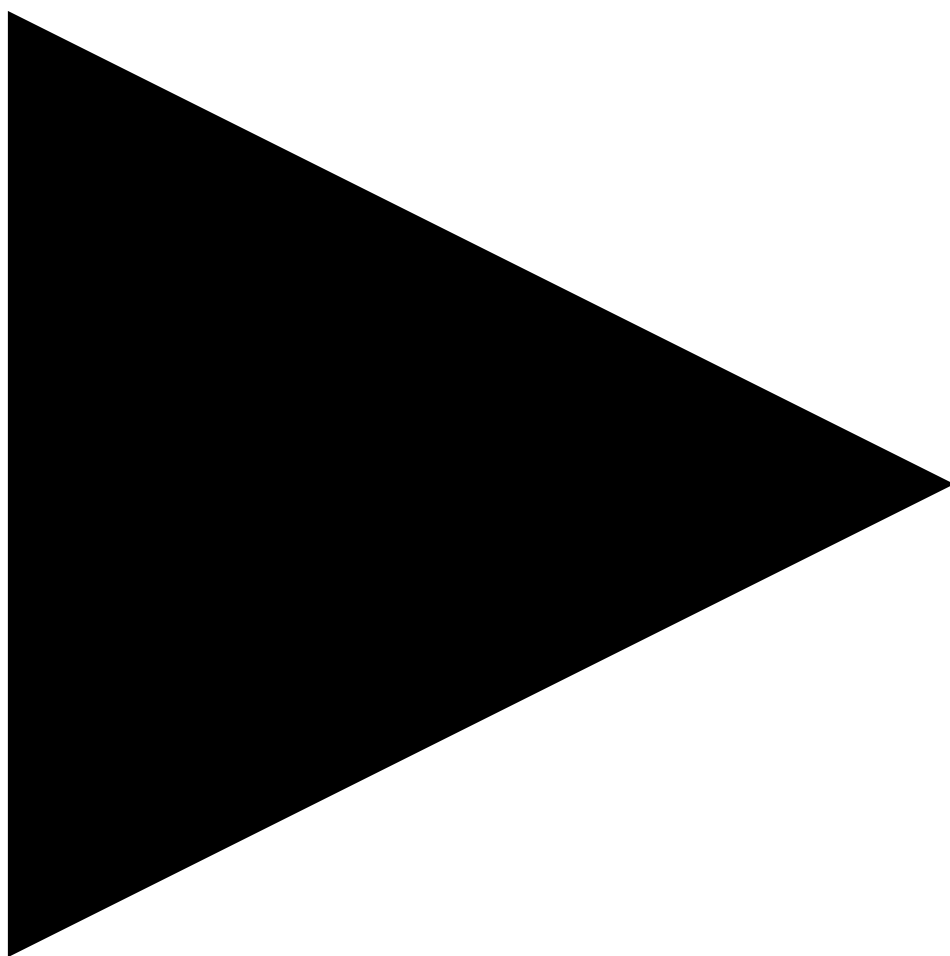


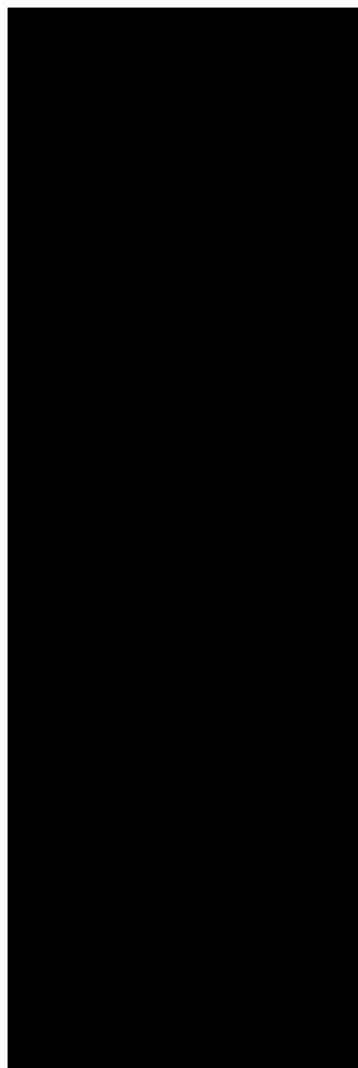
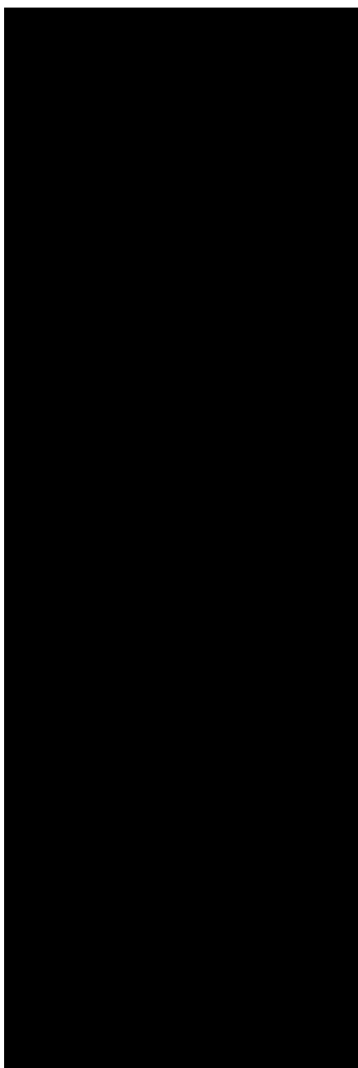
Finnish IT services and enterprise cloud hosting provider Tietoevry has suffered a ransomware attack impacting cloud hosting customers in one of its data centers in Sweden, with the attack reportedly conducted by the Akira ransomware gang.

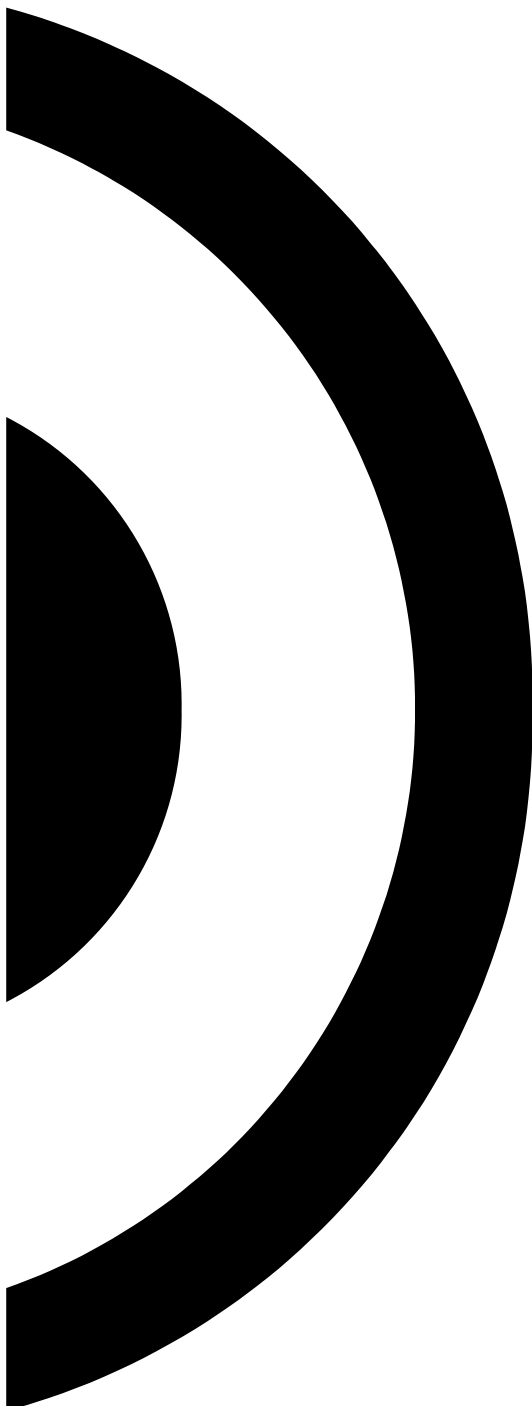
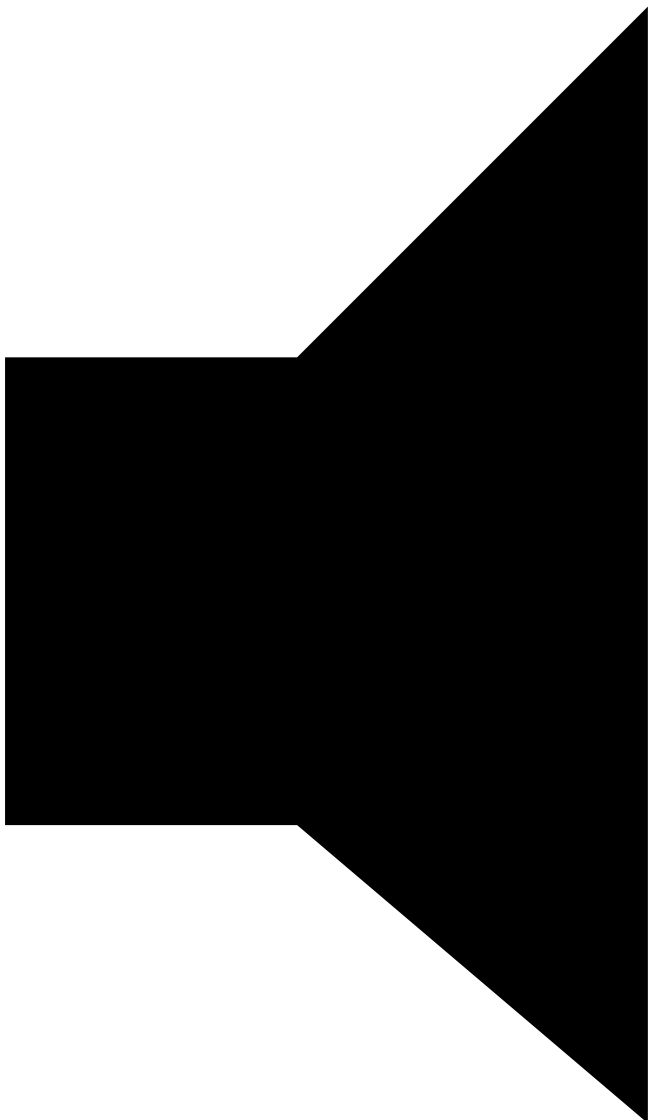
Tietoevry is a Finnish IT services company offering managed services and cloud hosting for the enterprise. The company employs approximately 24,000 people worldwide and had a 2023 revenue of \$3.1 billion.

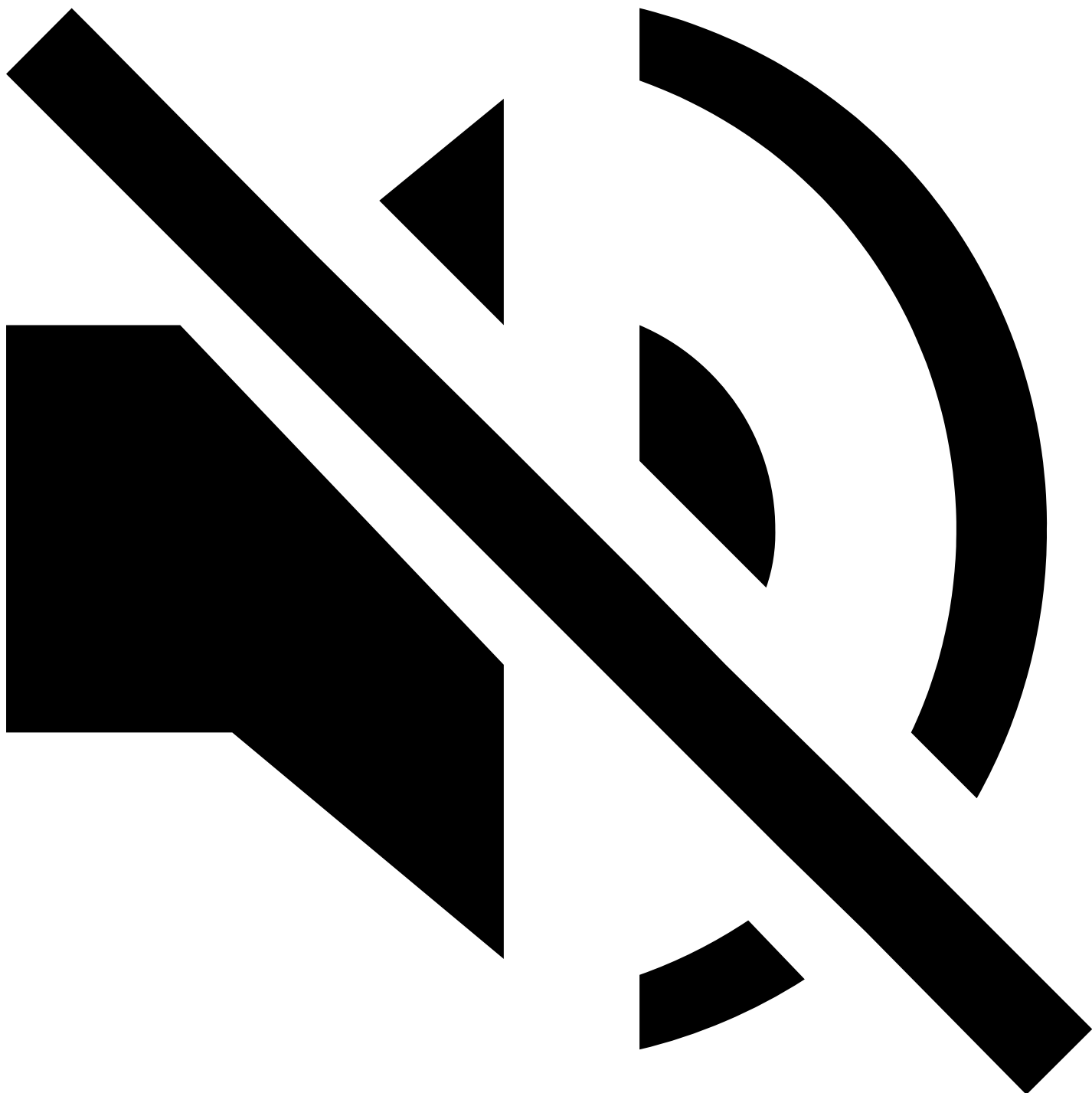
Tietoevry confirmed today that the ransomware attack occurred Friday night into Saturday morning and has impacted only one of their data centers in Sweden.

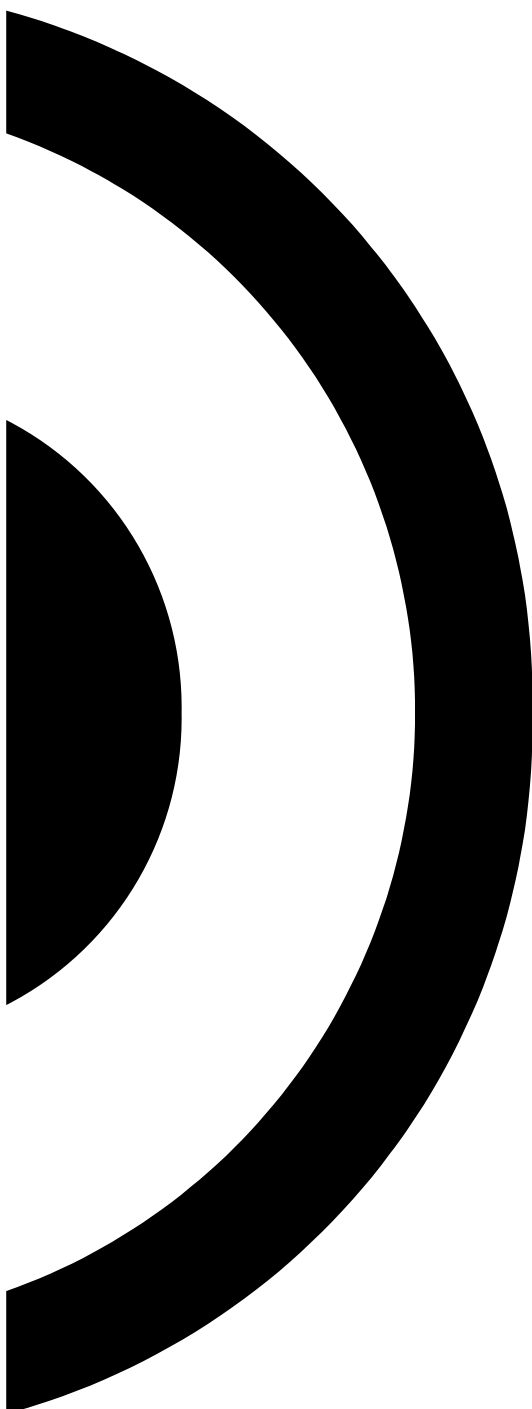
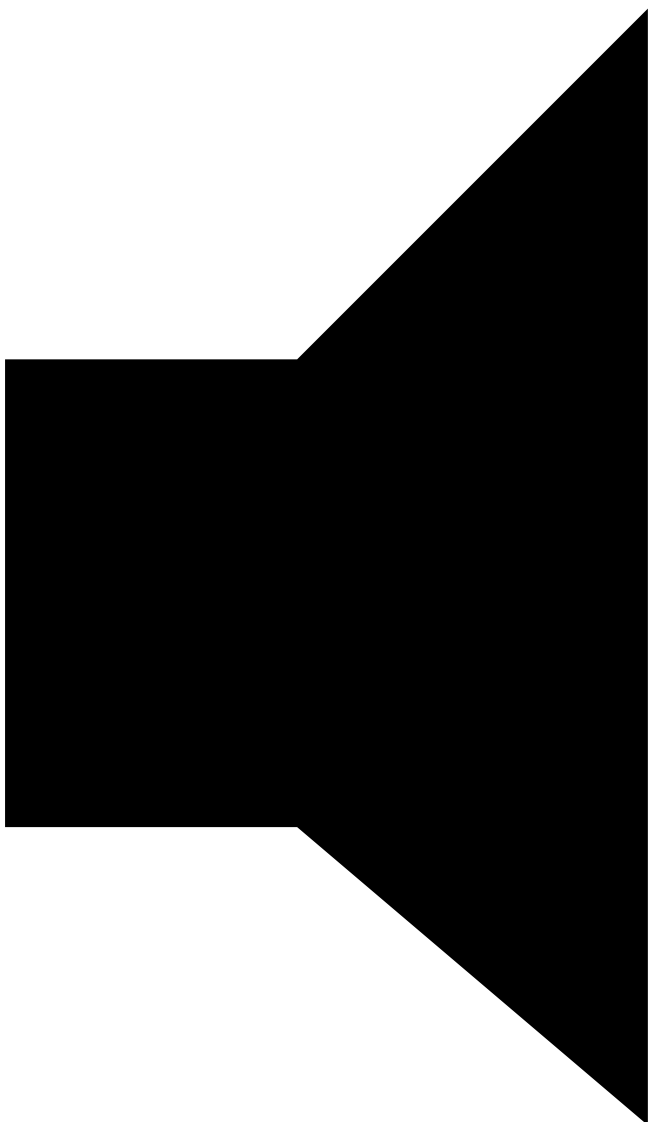
AD

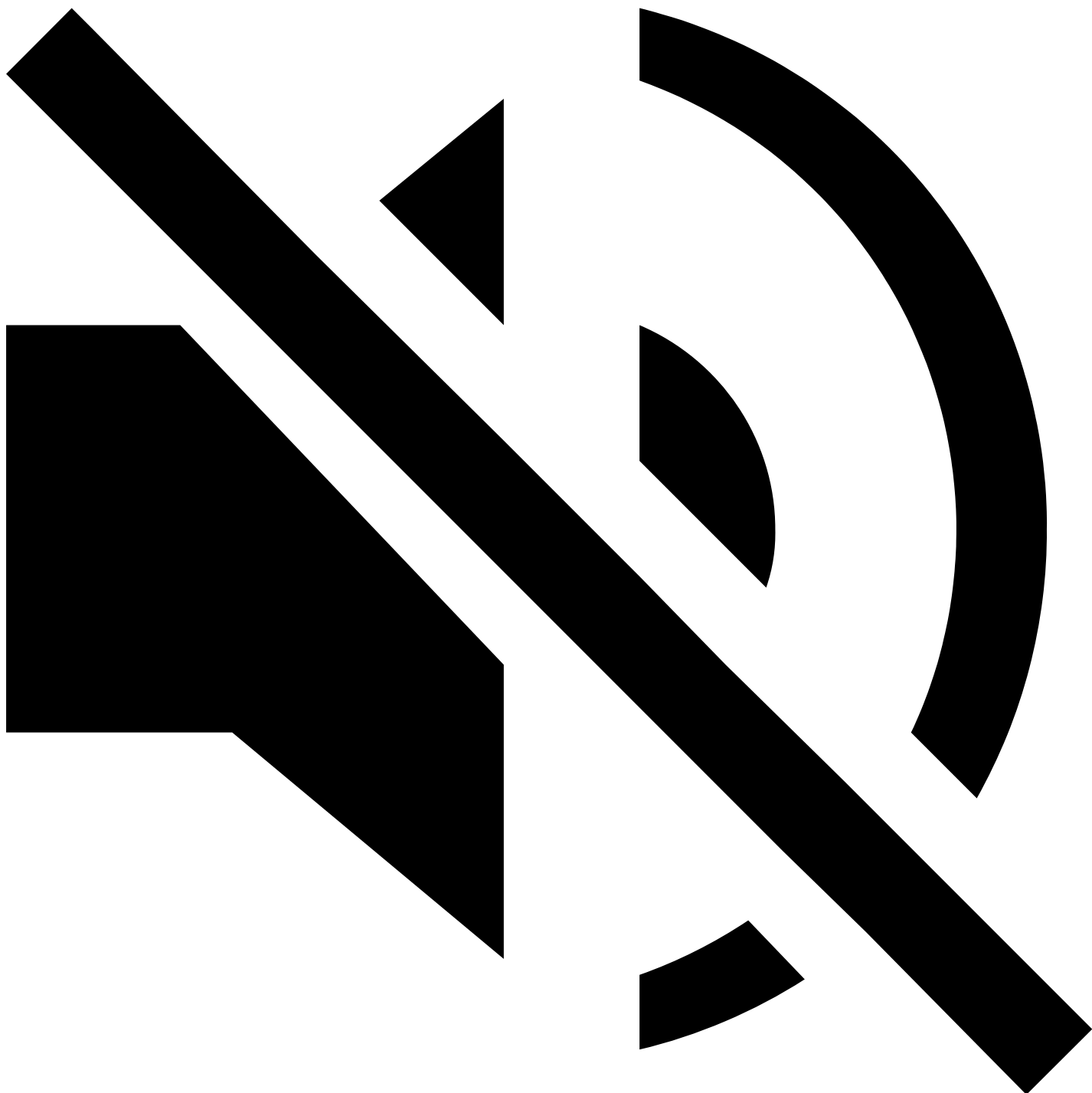


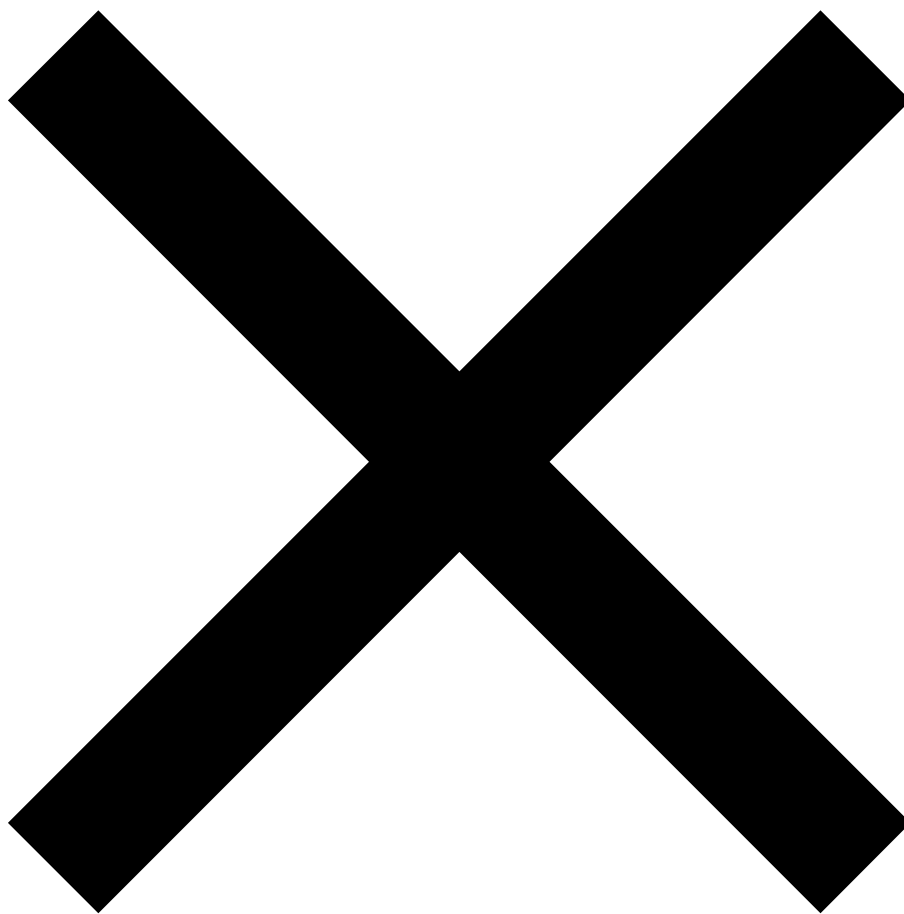





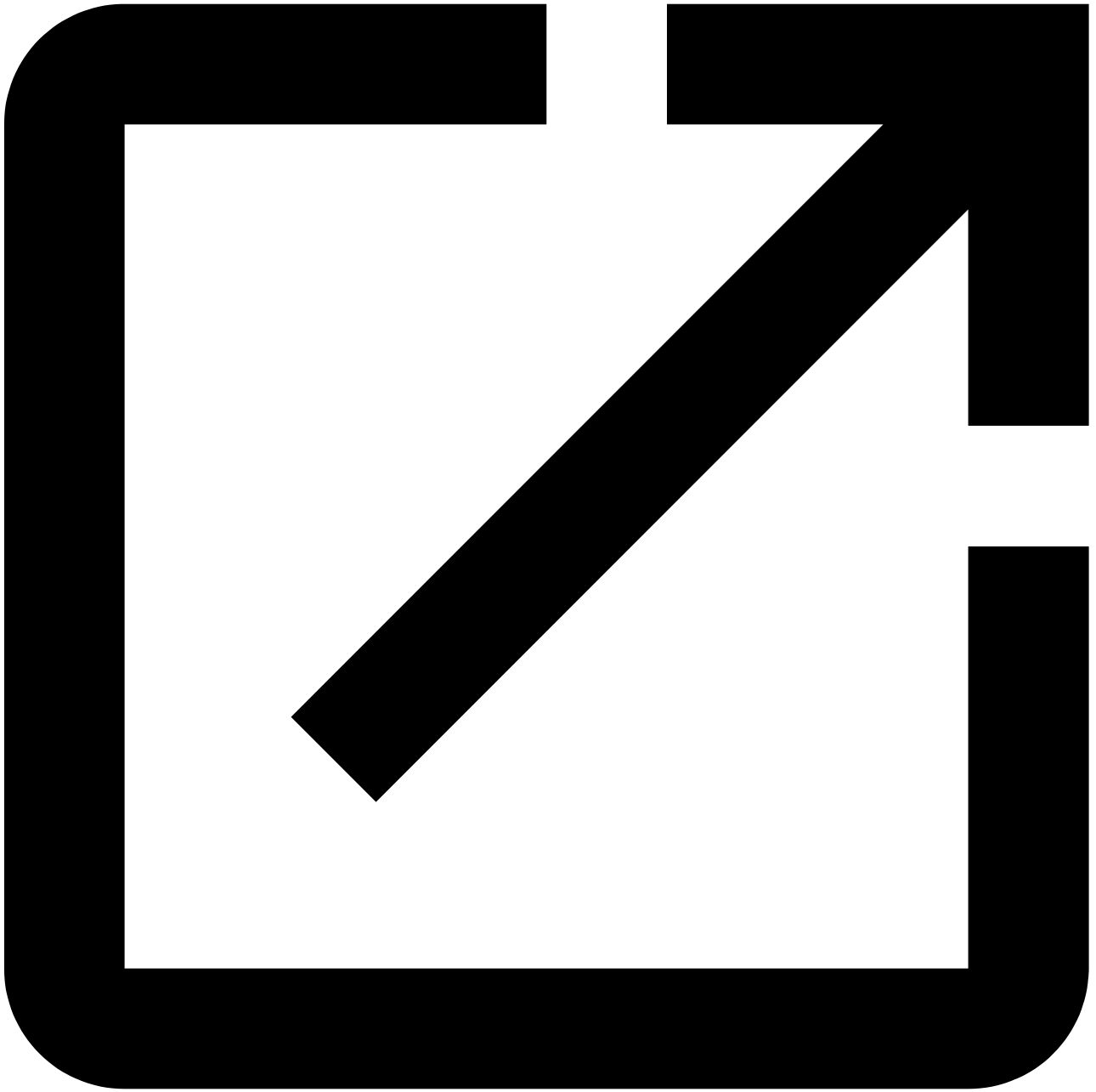




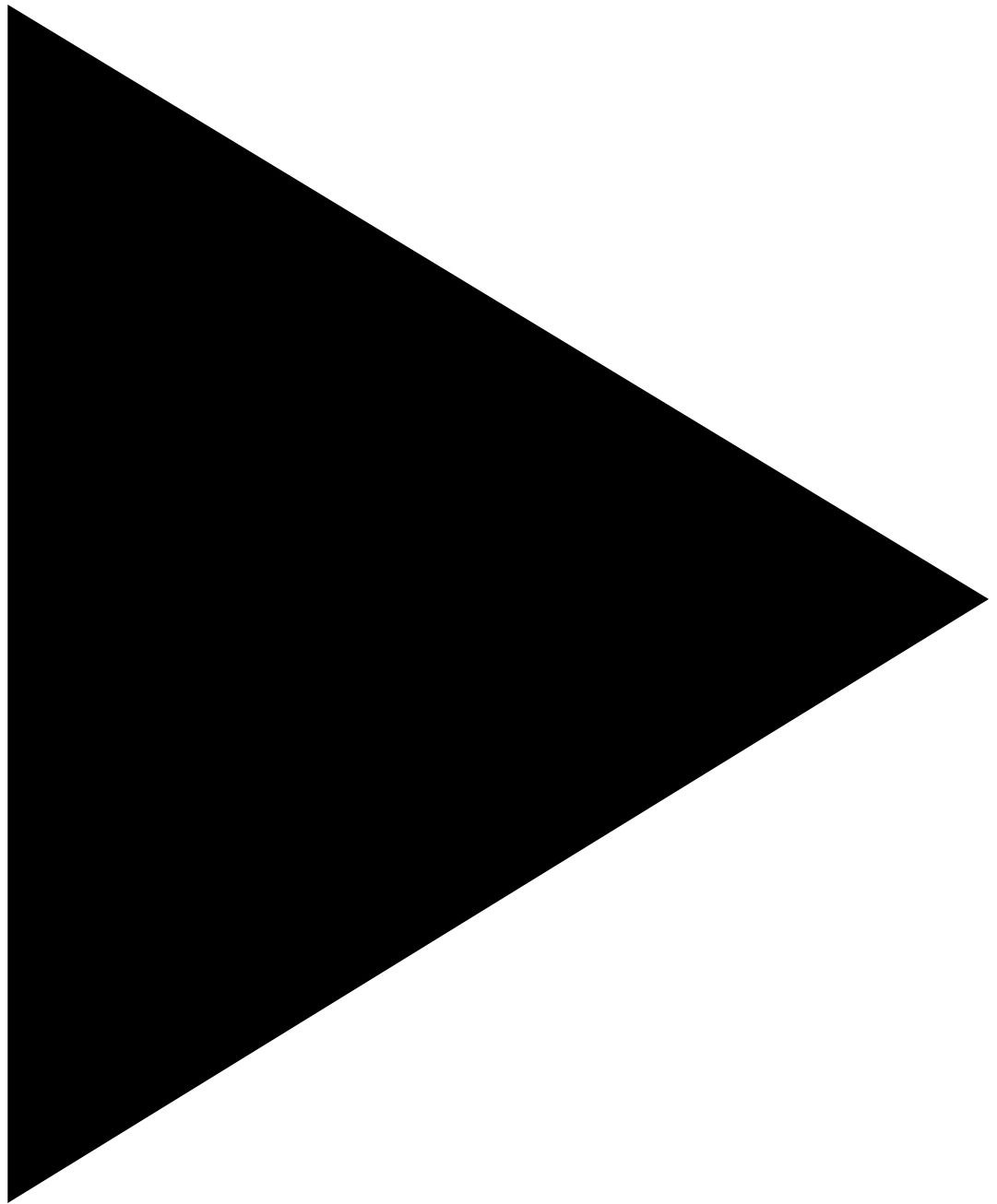




Continue watching after the ad  Loading Pods



Visit Advertiser website[GO TO PAGE](#)

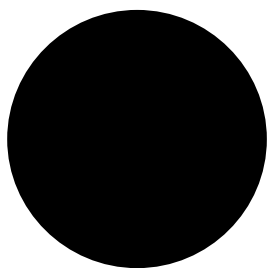
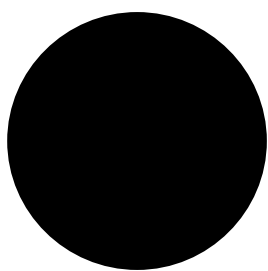
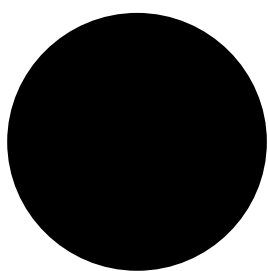


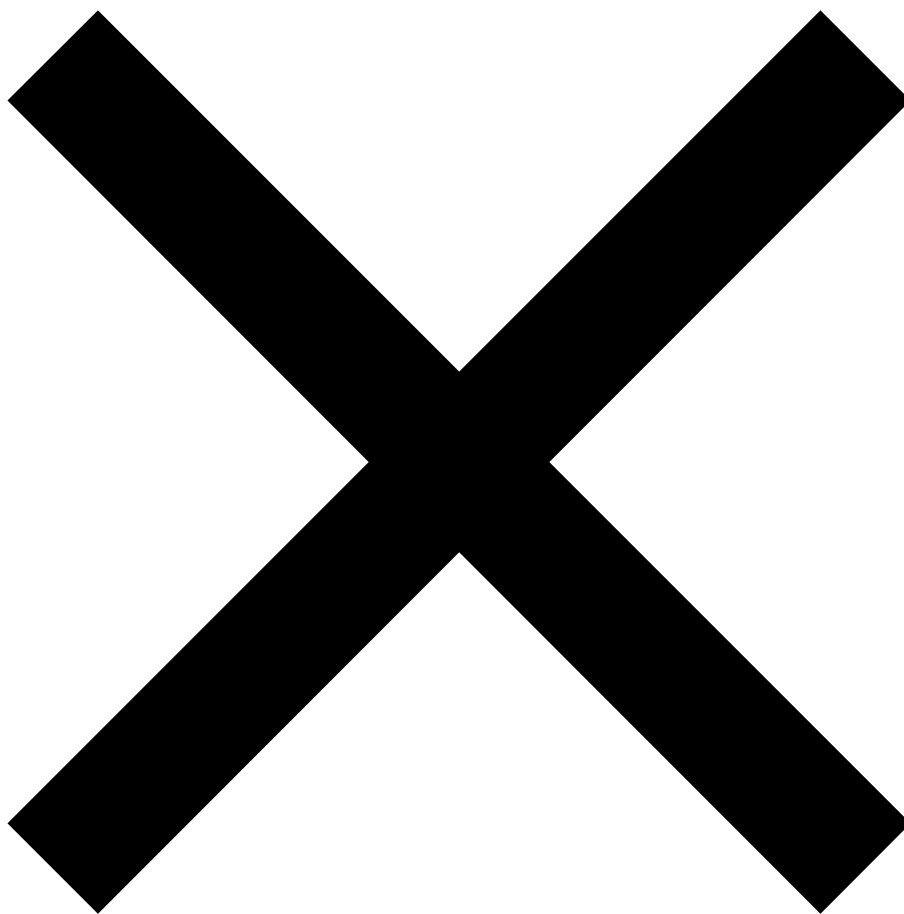
bleepingcomputer

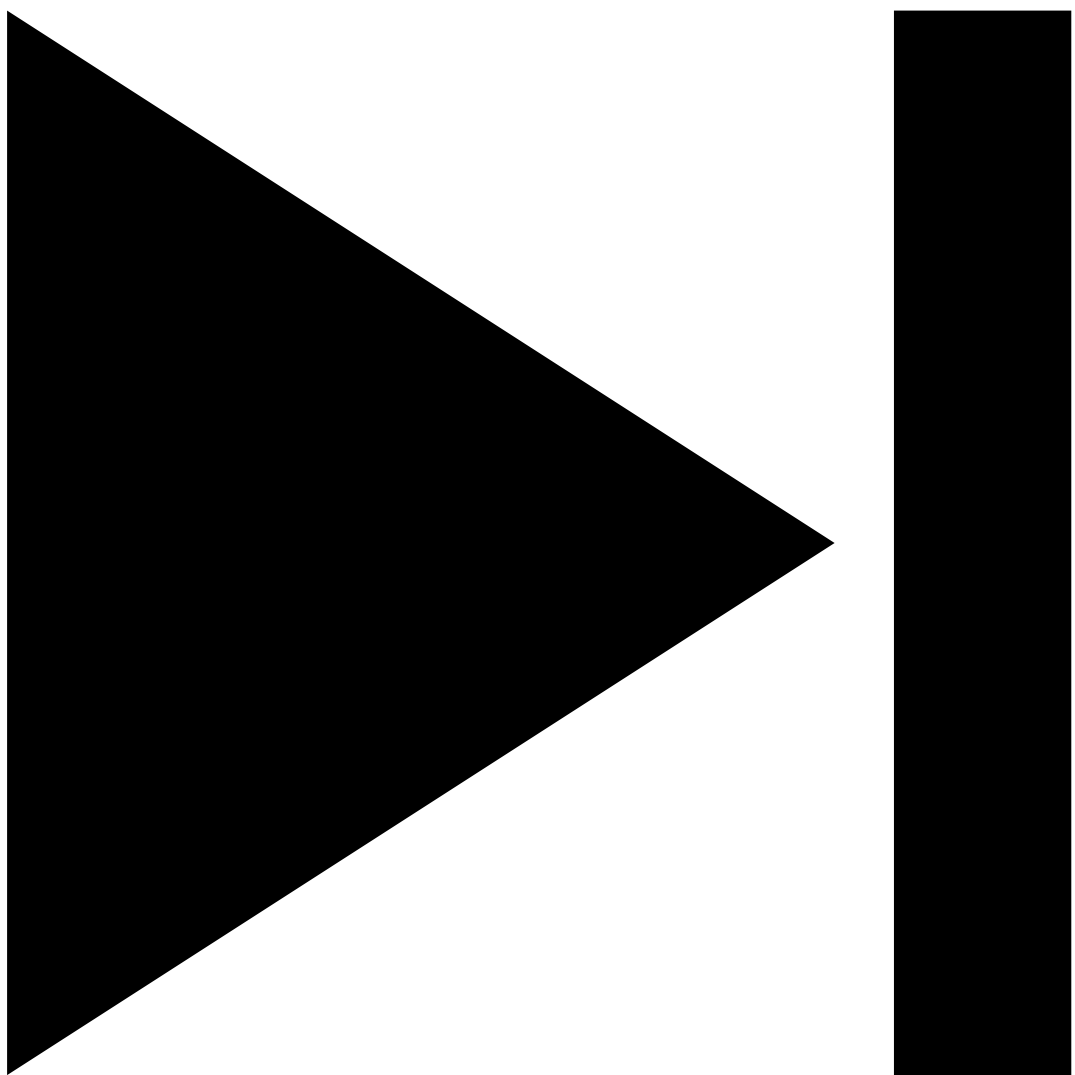
From a bleeping computer to a working computer

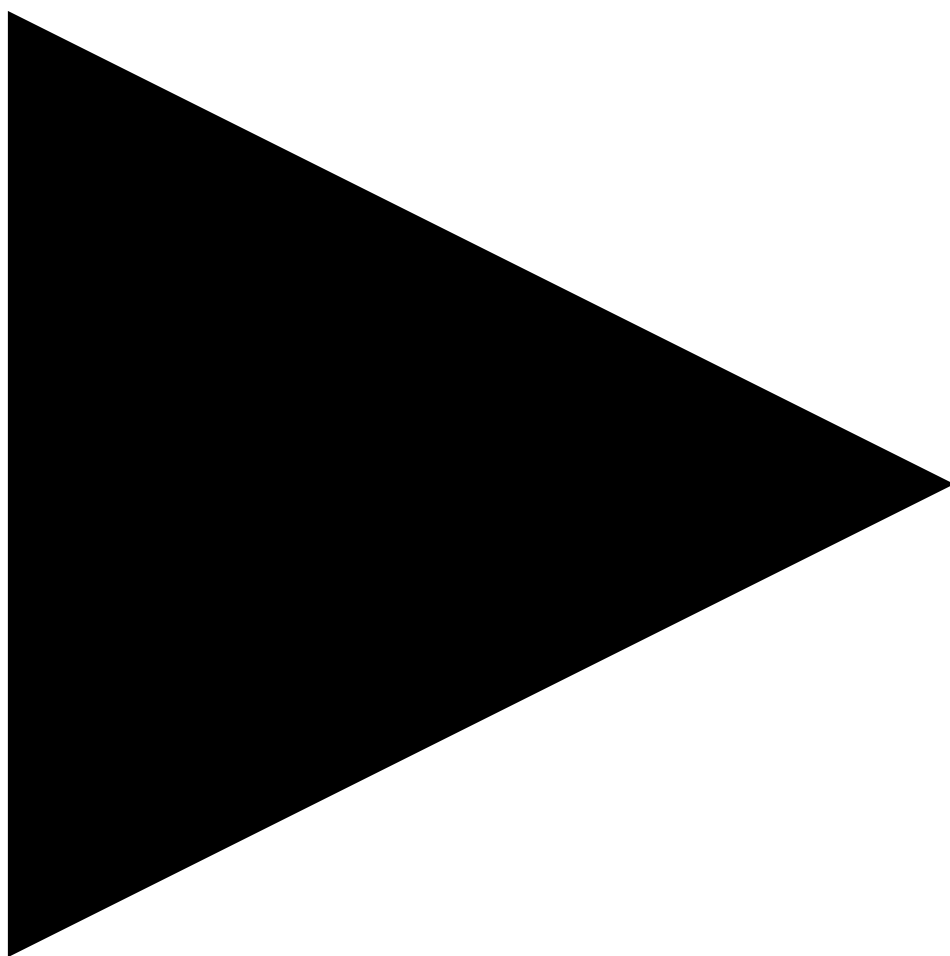
PLAY

Top Stories

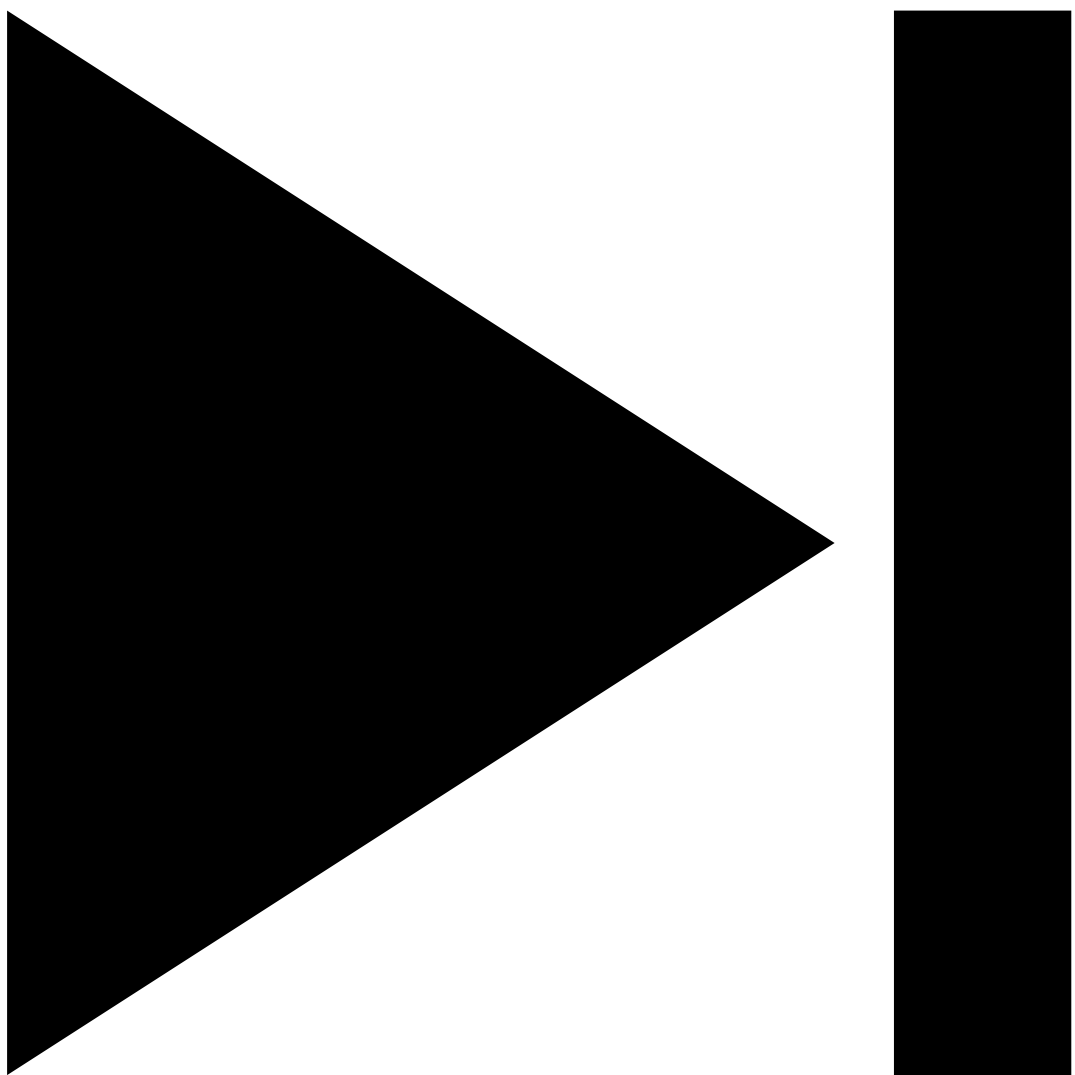


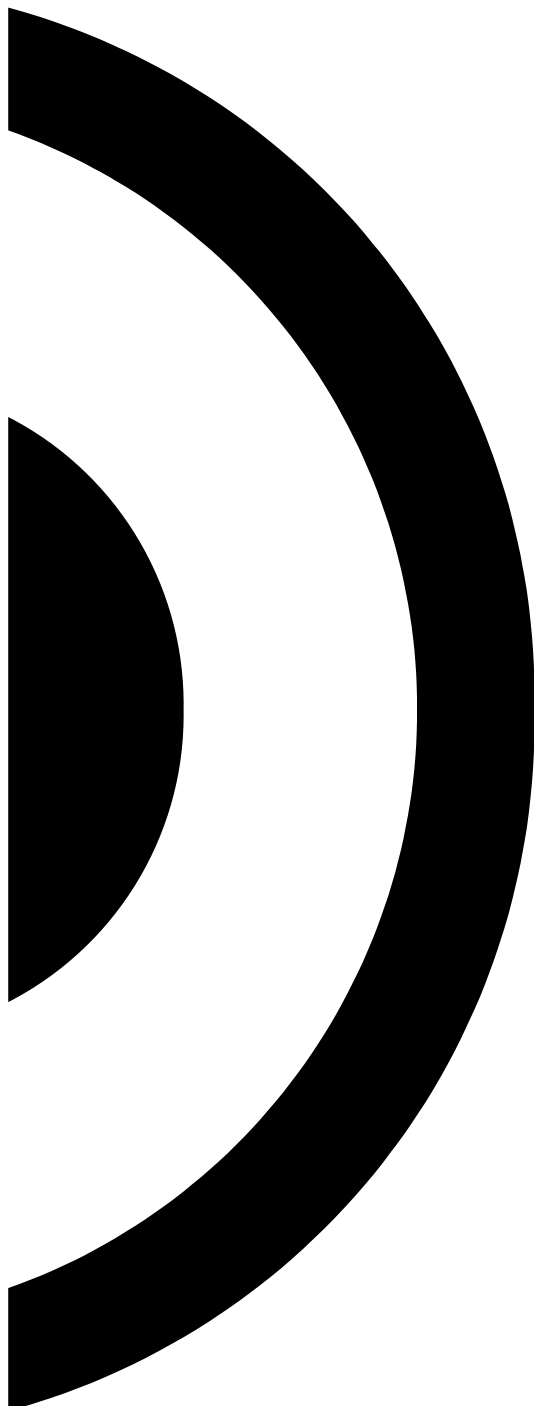
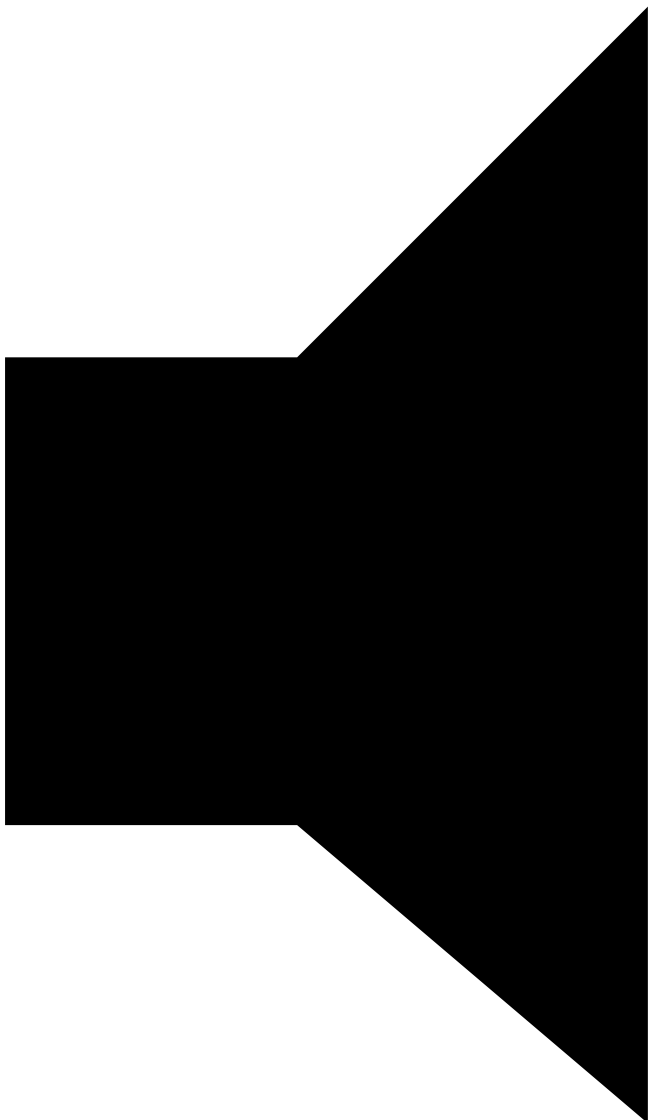


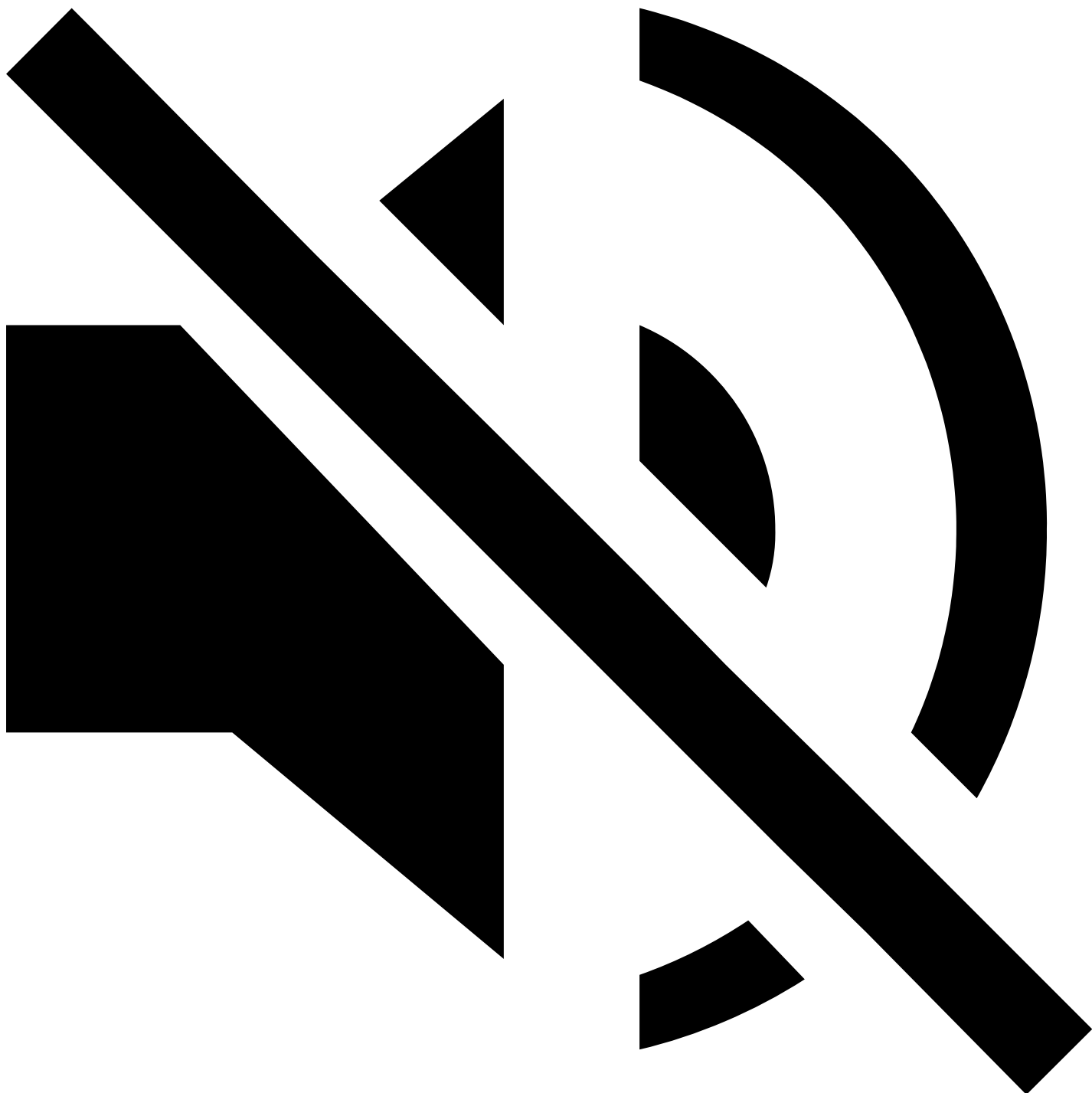




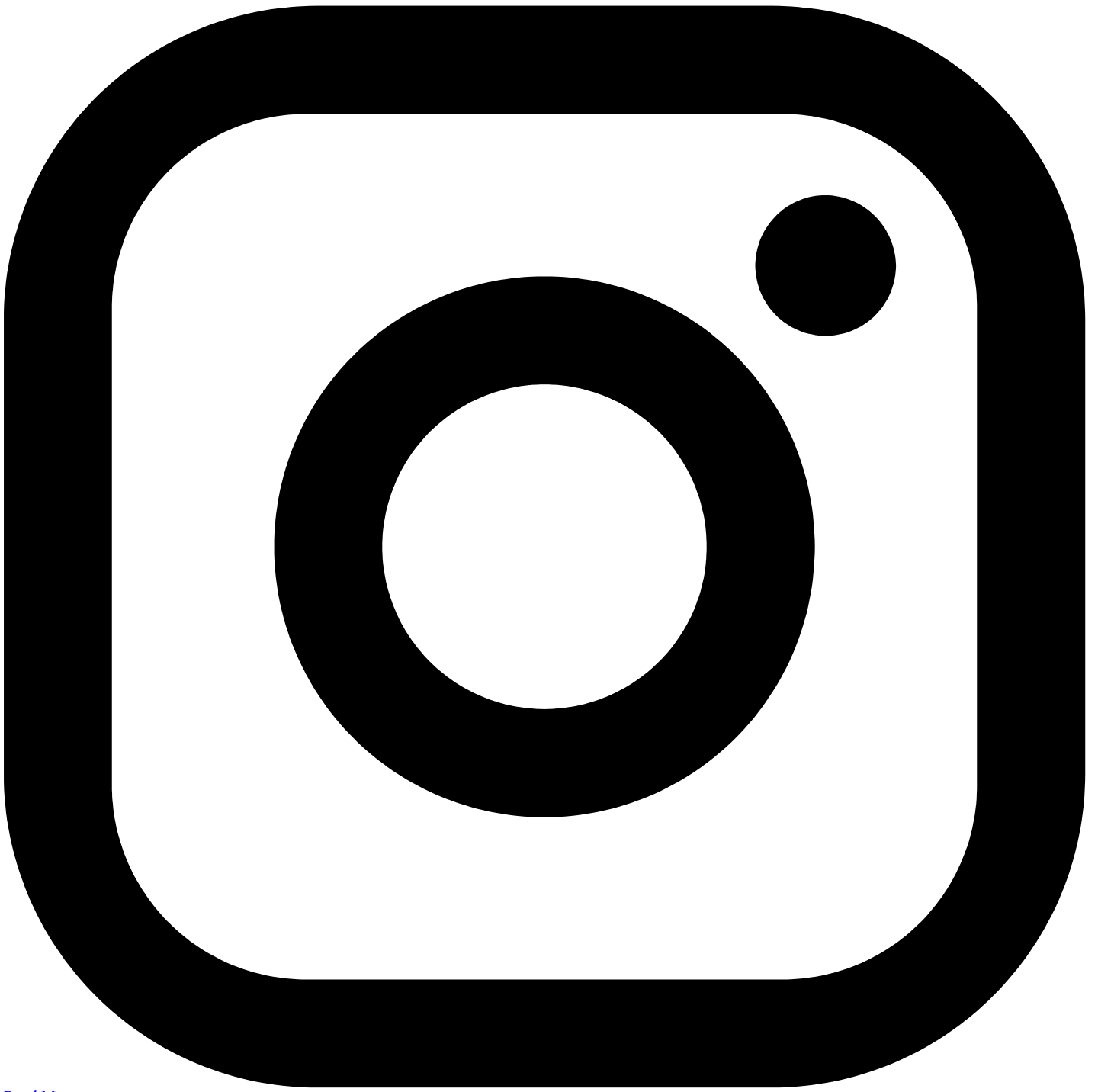




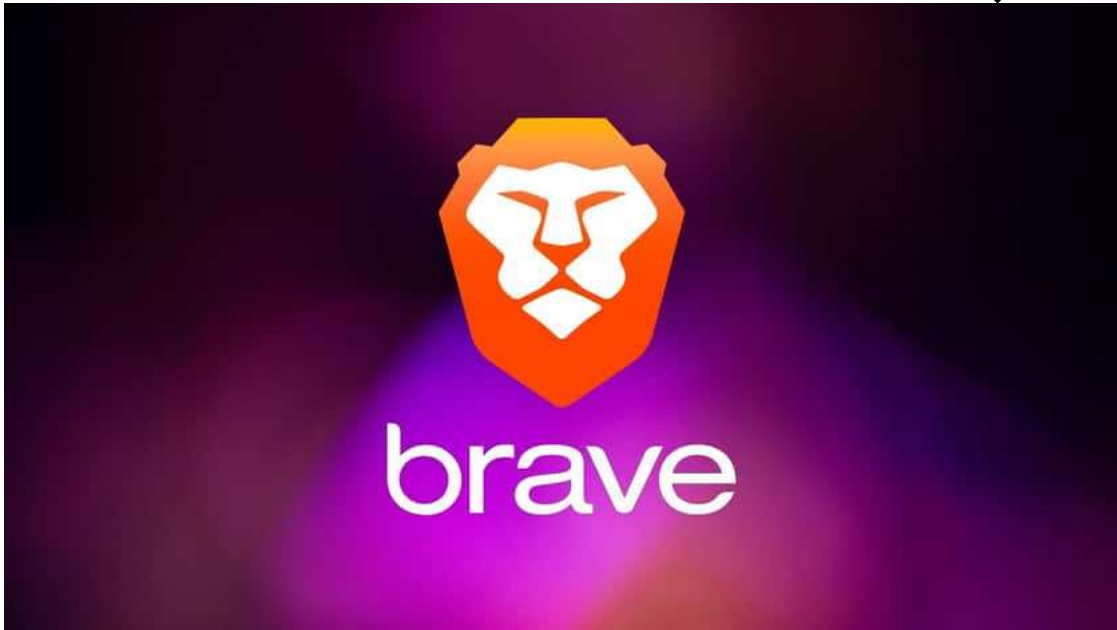
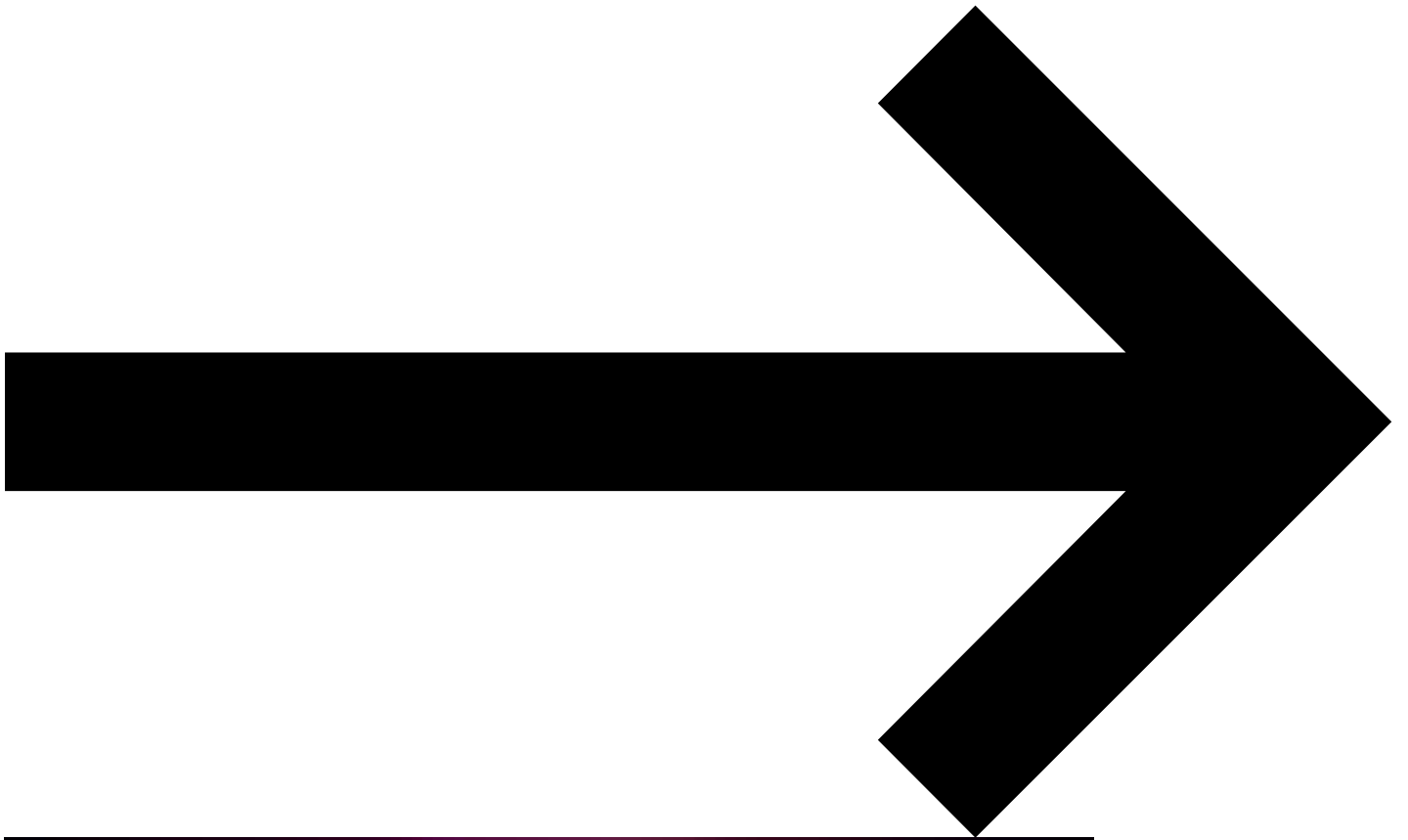


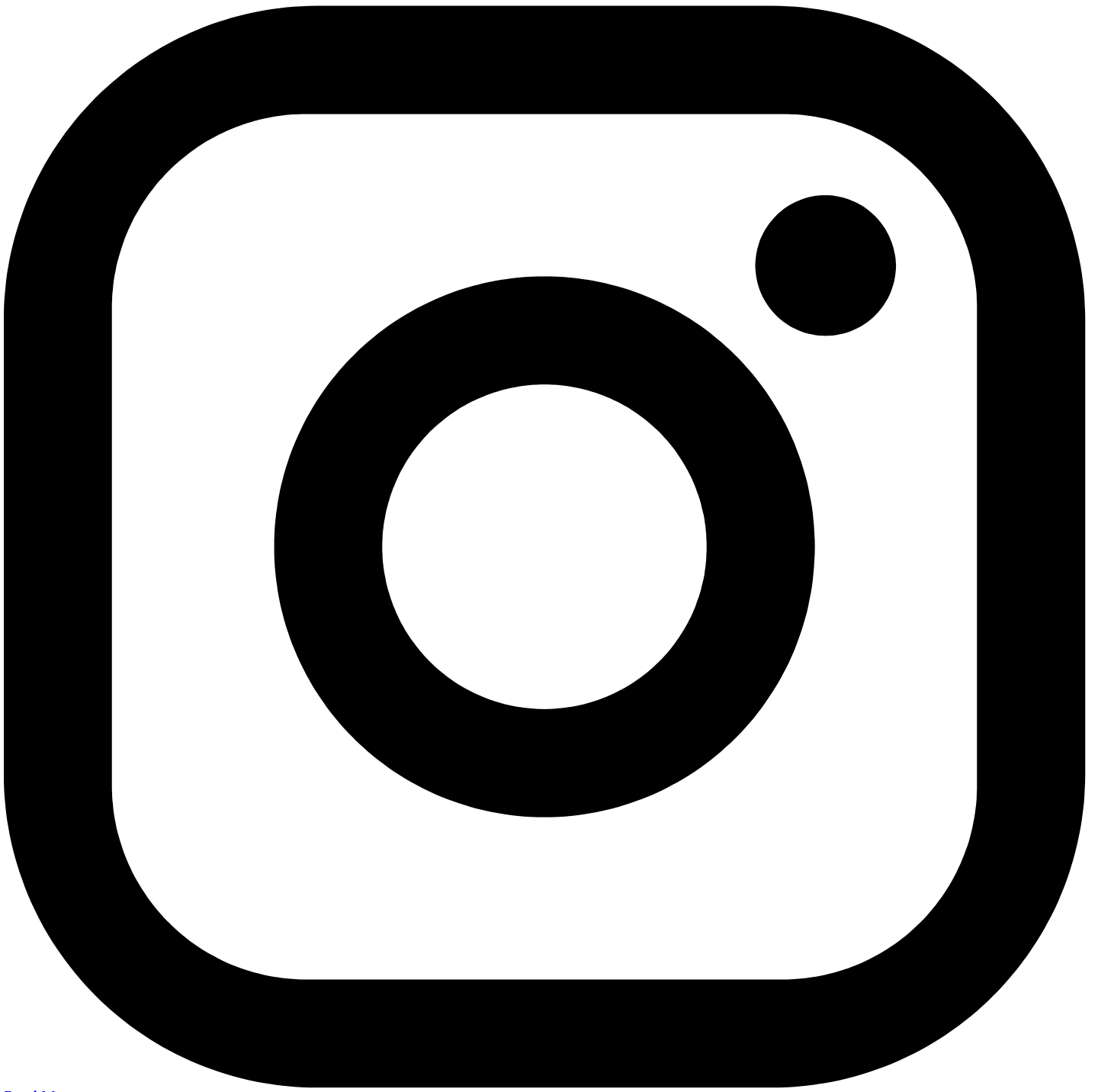




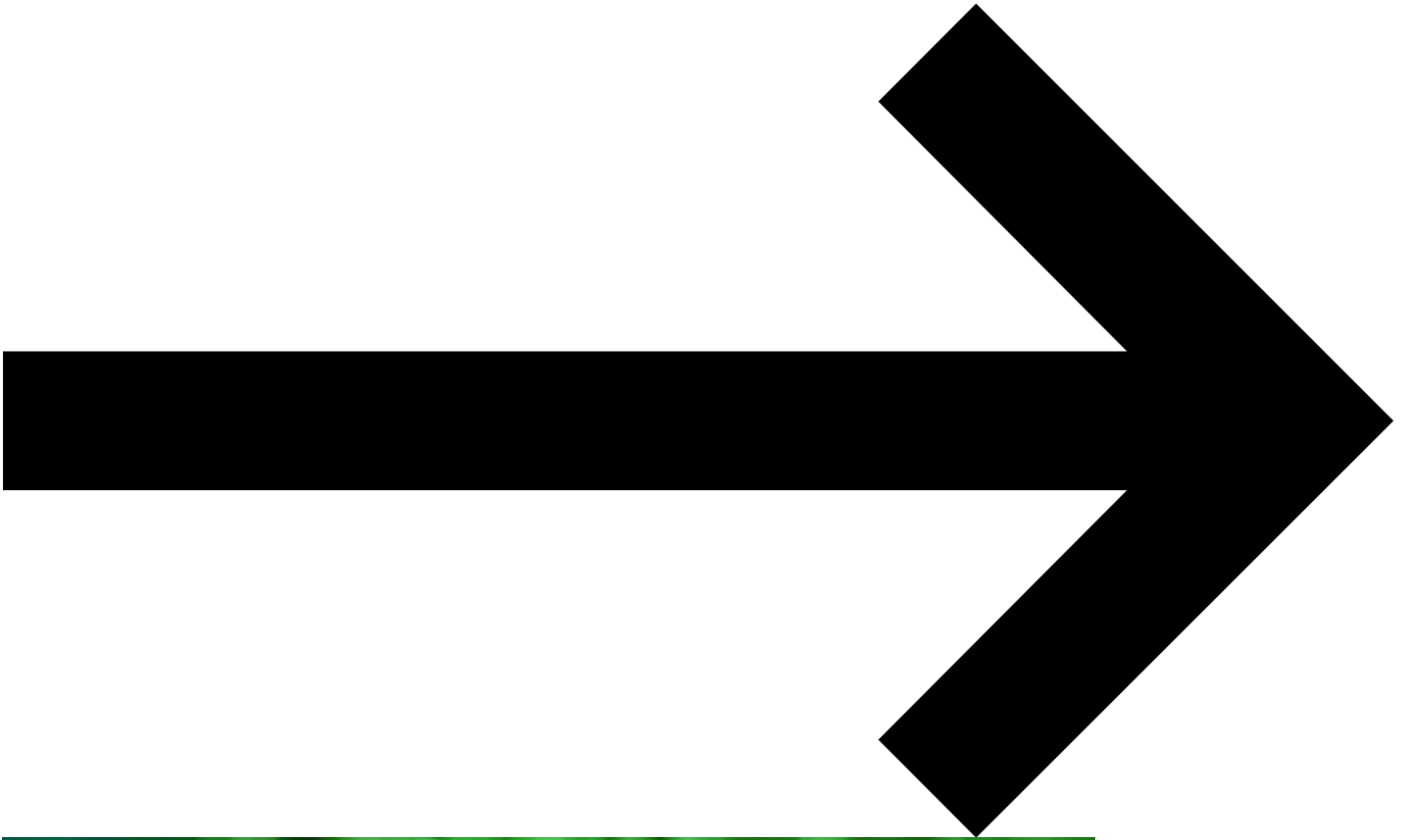


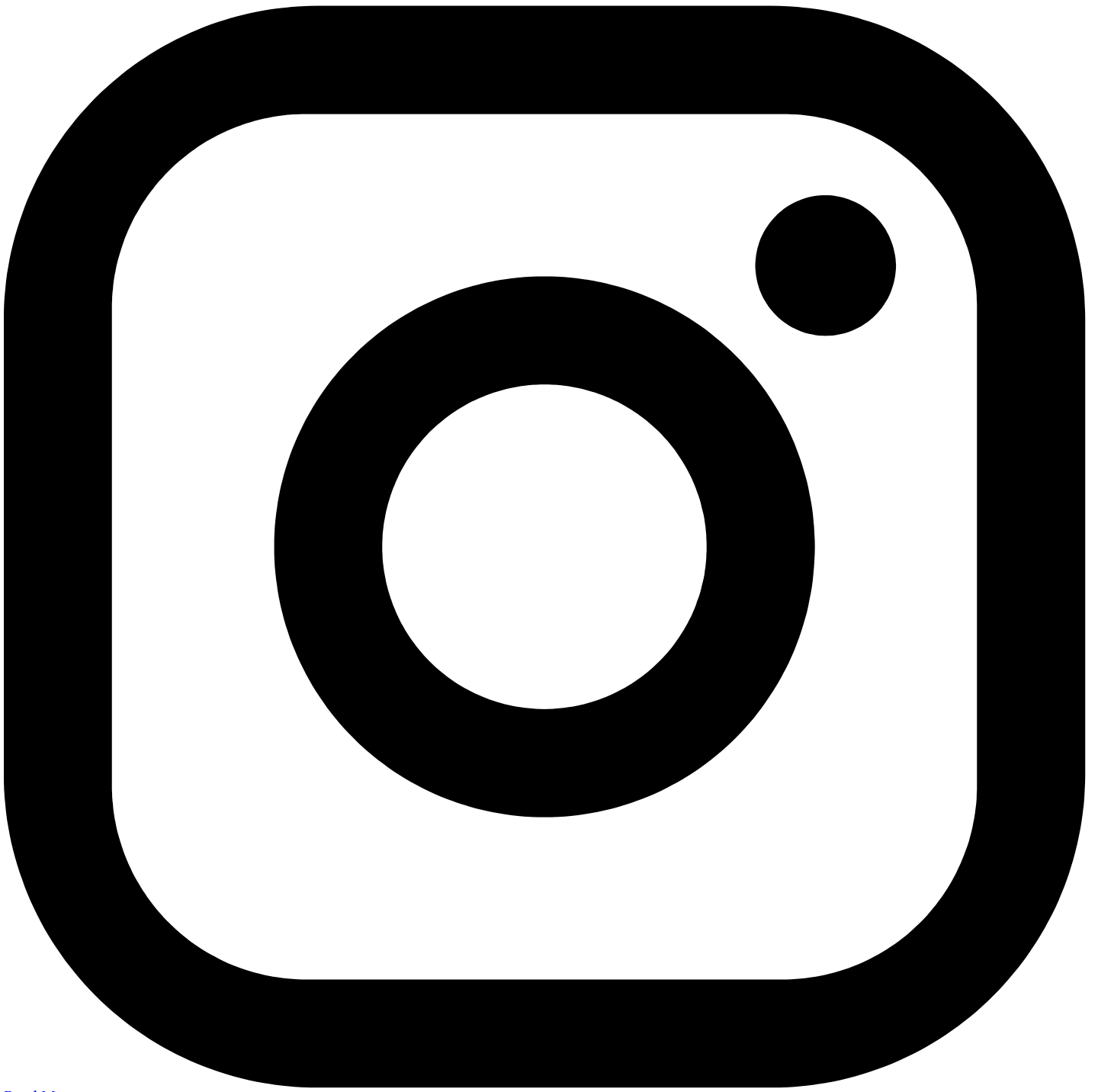
[Read More](#)



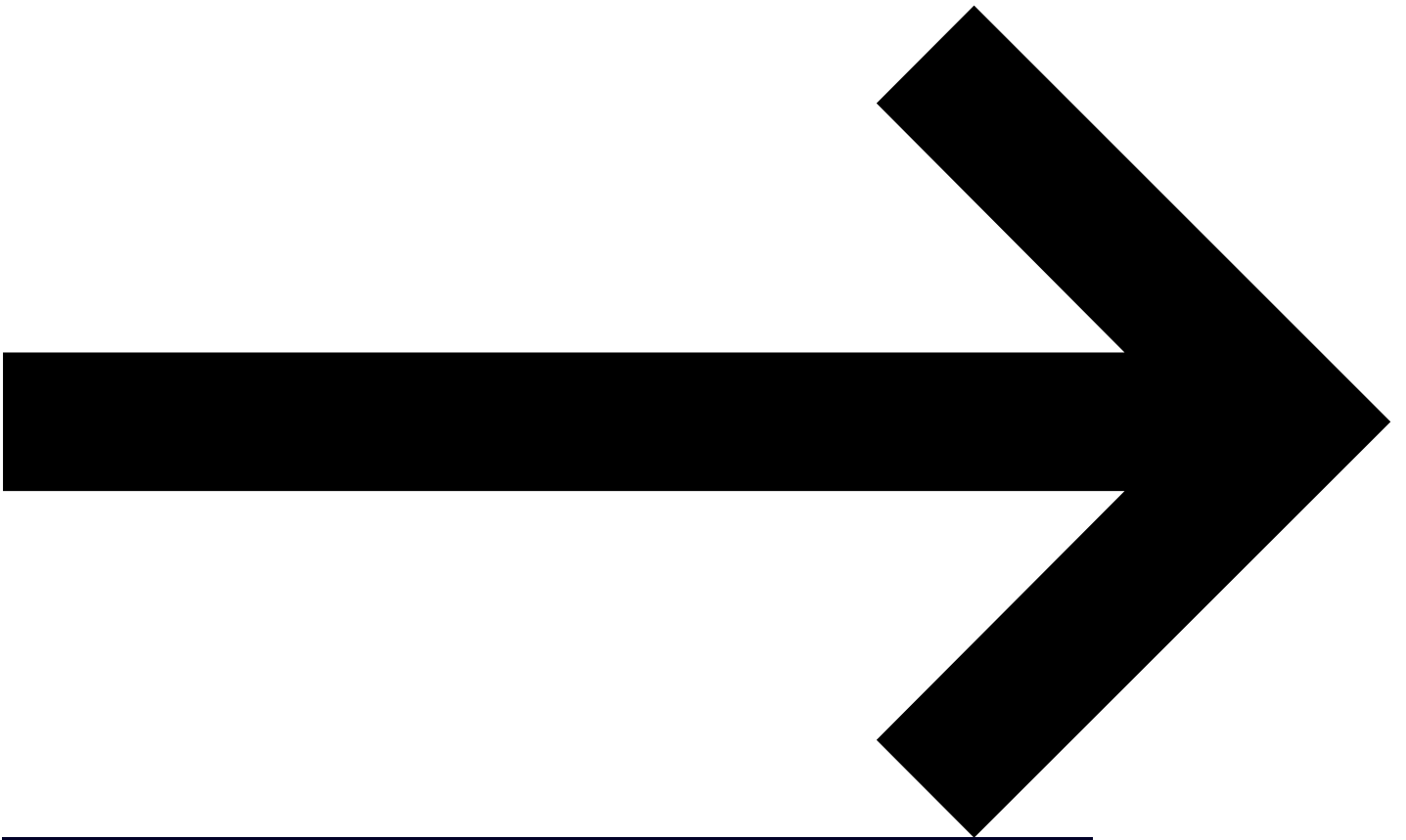


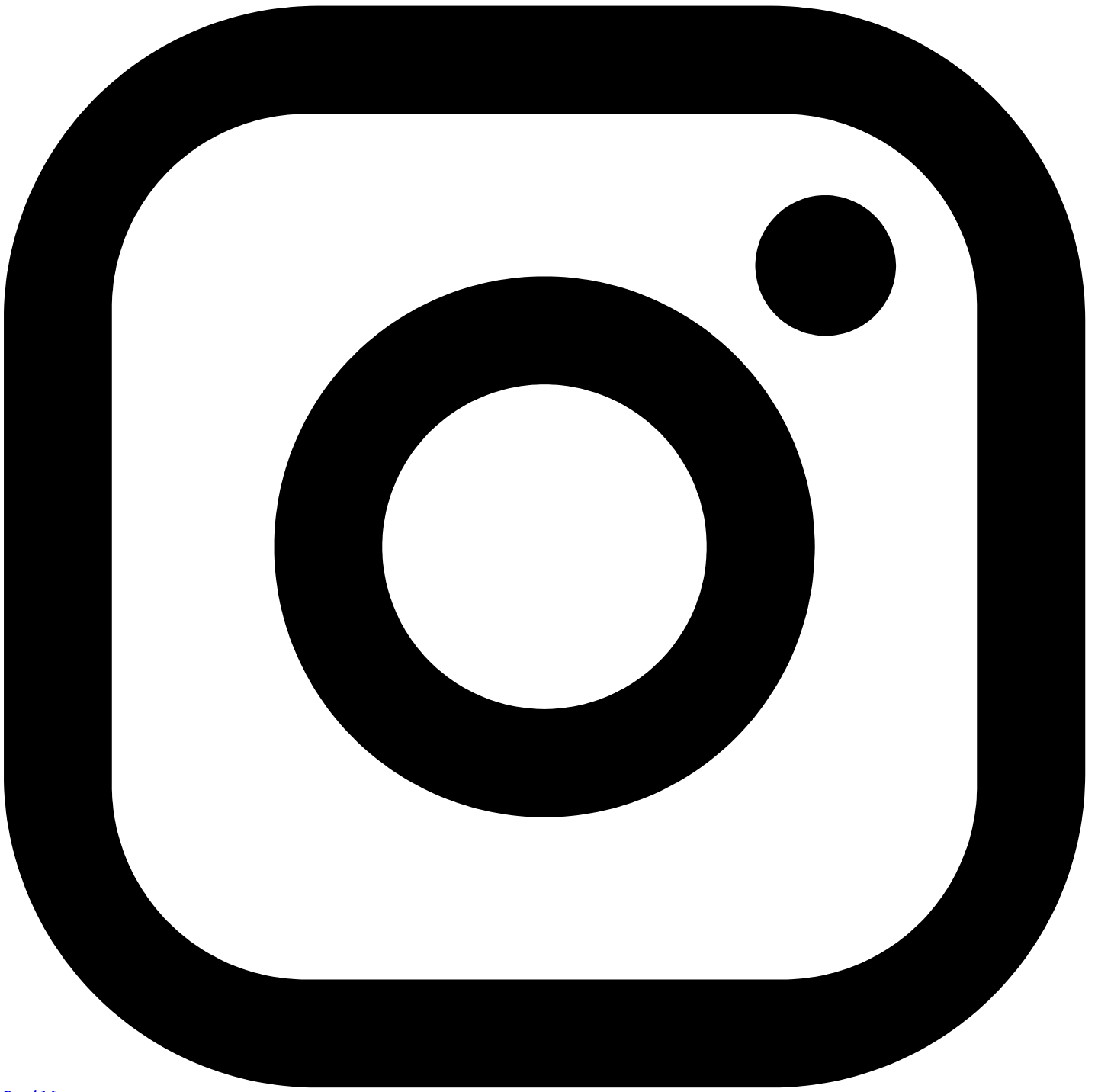
[Read More](#)



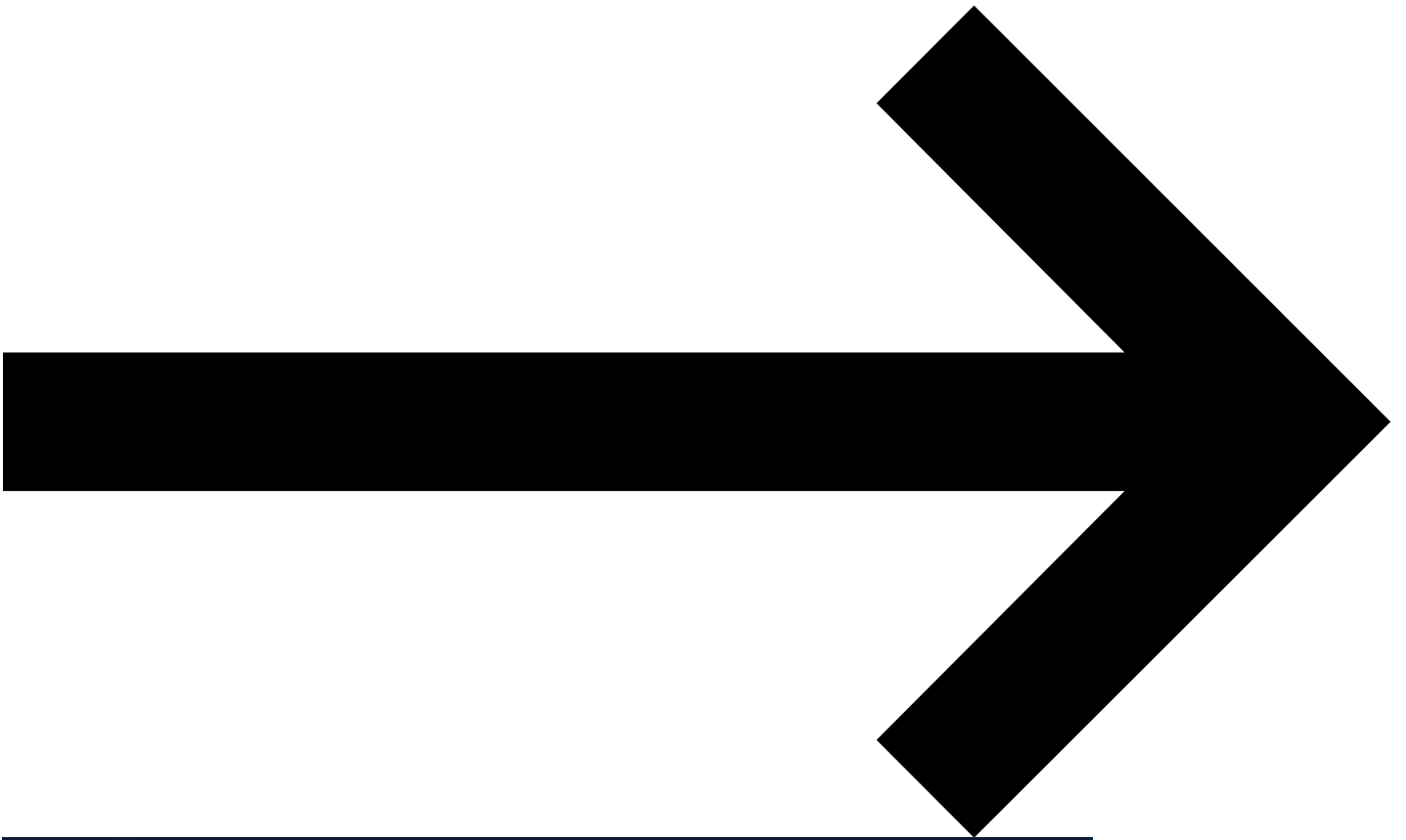


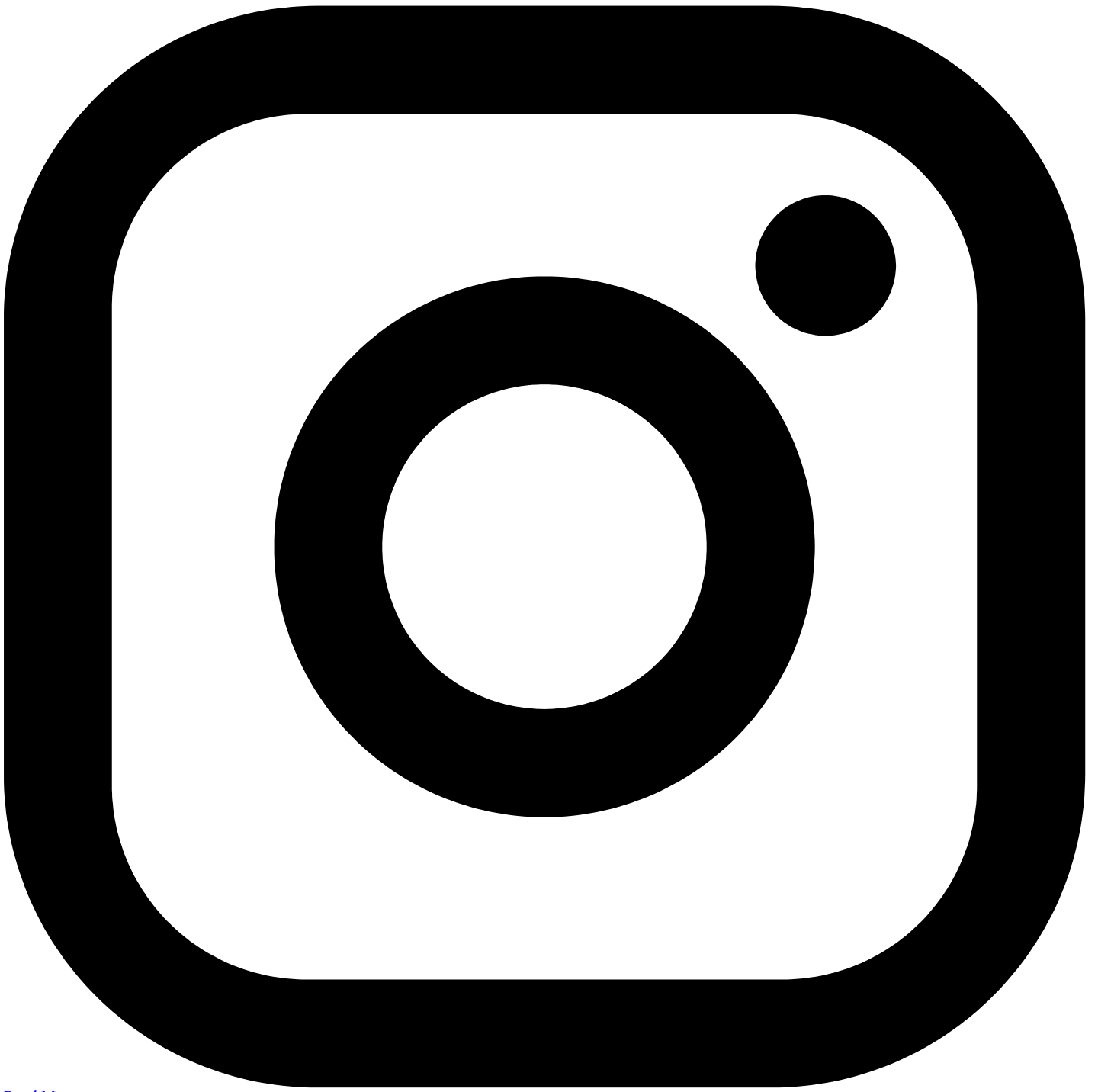
[Read More](#)





[Read More](#)

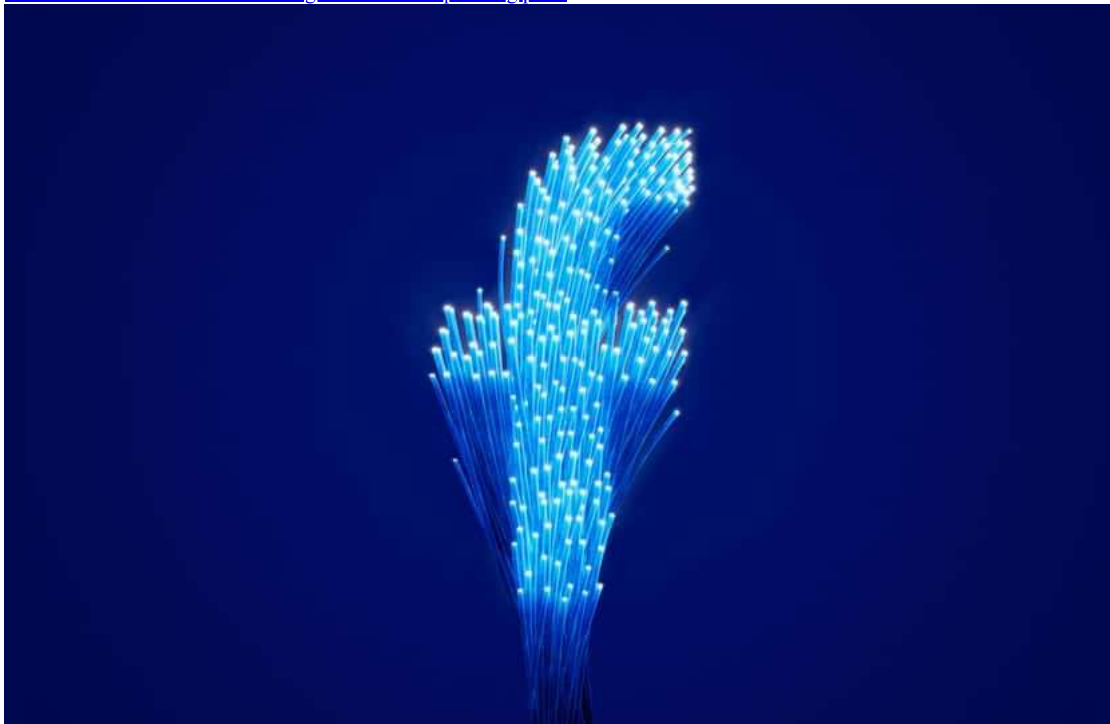




[Read More](#)



[Watch out for "I can't believe he is gone" Facebook phishing posts](#)



"The attack was limited to one part of one of our Swedish datacenters, impacting Tietoevry's services to some of our customers in Sweden," explains a press statement from Tietoevry.

"Tietoevry immediately isolated the affected platform, and the ransomware attack has not affected other parts of the company's infrastructure."

BleepingComputer has learned that this data center is used for the company's enterprise-managed cloud hosting service, leading to outages for multiple customers in Sweden.

The company says that they are in the process of restoring infrastructure and services but that customers still remain impacted as they bring servers back online.

"Tietoevry is following a well-tested methodology in order to restore infrastructure and services. The work is conducted in a planned sequence to ensure correct handling of customer data," continues the [press statement](#).

"Time schedule will also vary somewhat depending on the customer, the solutions in question and the related data restoring needs."

BleepingComputer has contacted Tietoevry for further information about the attack but was only told that the attack "impacted a specific section of one of Tietoevry's data centers located in Sweden."

Tietoevry [previously suffered a ransomware attack](#) in 2021 that forced them to disconnect clients' services.

If you have any information on this attack or other cyberattacks, you can contact us securely on Signal at +1 (646) 961-3731, via email at tips@bleepingcomputer.com, or by using our [tips form](#).

Attack causes widespread outages

BleepingComputer has learned that the ransomware attack encrypted the company's virtualization and management servers used to host the websites or applications for a wide range of businesses in Sweden.

Sweden's largest cinema chain, [Filmstaden](#), has confirmed that they are among those impacted by the attack, preventing online purchases of movie tickets through the website or mobile app.



Message on Filmstaden's website warning of the IT outage

Source: BleepingComputer

Other companies impacted by the attack include discount retail chain [Rusta](#), raw building materials provider [Moelven](#), and farming supplier Grangnården, which was forced to [close its stores](#) while IT services are restored.

The outage is also impacting Tietoevry's managed Payroll and HR system, Primula, which is used by the government, universities, and colleges in Sweden.

Impacted universities and colleges in the country include the [Karolinska Institutet](#), [SLU](#), [University West](#), Stockholm University, Lunds Universitet, and Malmö University.

The Primula outage has also impacted numerous government agencies and municipalities in Sweden, including the [Statens servicecenter](#), the [Vellinge municipality](#), [Bjuv's municipality](#), and [Uppsala County](#).

For Uppsala the outage is more significant as it also impacts the region's health care record system.

Akira ransomware allegedly behind attack

BleepingComputer has been told that the Akira ransomware operation is behind the attack on Tietoevry, coming soon after the Finnish government warned about their ongoing attacks against companies in the country.

The [Akira ransomware operation](#) launched in March 2023 and quickly began breaching corporate networks worldwide in double-extortion attacks.

The Finnish National Cyber Security Center (NCSC) [disclosed this month](#) that there were 12 reported cases of Akira ransomware attacks in 2023, with the majority happening late in the year.

"The incidents were particularly related to weakly secured Cisco VPN implementations or their unpatched vulnerabilities. Recovery is usually hard," warned the Finnish NCSC.

In August, BleepingComputer reported on the [Akira ransomware gang breaching Cisco VPN accounts](#) that weren't protected by multi-factor authentication to gain access to internal corporate networks.

Once the threat actors breach a network, they spread laterally to other devices while stealing corporate data. Once all data has been stolen and they gain administrative privileges, the threat actors encrypt files on the network.

Cisco told BleepingComputer at the time that customers should configure MFA on all VPN accounts and send logging data to a remote syslog server.

Using a remote syslog server, even if the threat actors clear logs on the Cisco router, they will still be accessible for analysis after a breach.

Related Articles:

[Finland warns of Akira ransomware wiping NAS and tape backup devices](#)

[Nissan Australia cyberattack claimed by Akira ransomware gang](#)

[Researchers link 3AM ransomware to Conti, Royal cybercrime gangs](#)

[Vans, North Face owner says ransomware breach affects 35 million people](#)

[TeamViewer abused to breach networks in new ransomware attacks](#)