ACS Publications
Most Trusted. Most Cited. Most Read.

Important Security Notification

Dear Valued ACS Customer,

We have reason to believe that your organization could potentially be targeted for a cyber-attack.

In the past month, ACS has experienced a significant increase in improper access to and downloading of its online journals as a result of serious, sophisticated and sustained attacks on information networks of research universities and their libraries worldwide. Over 150 academic libraries located around the world have already experienced large-scale illegitimate access and session requests to their campus and library networks.

The abnormal activity we have experienced over the past month includes thousands of fraudulent session requests coming through academic networks, in which hundreds of articles have been downloaded in each session. These attacks are highly sophisticated and agile—they adjust their method of attack based on the security and usage monitoring tools they encounter.

From our interactions with academic institutions that have been victim to these security breaches, it is clear that an external party, or parties, has fraudulently obtained institutional passwords and user IDs. Once they gain access to academic networks using the fraudulently obtained credentials, sophisticated robotic download engines are able to download hundreds of articles in minutes. This type of security breach compromises your institution's networked information infrastructure, putting other confidential personal, research and financial data at risk, as well licensed content from ACS and other information providers.

Action you can take

Since it is not clear when or where new attacks will come from, we urge you to review both your own security protocols as well as your planned response and investigation strategy.

As the guardian of more than 100 years of published scientific articles, ACS has a positive obligation to protect the scientific record. ACS takes all theft of intellectual property very seriously. Consequently we are urgently revising our own capabilities and protocols on how we detect and prevent these intrusions, and we are upgrading the steps we require to restore access.

Actions we are taking

To help protect both your institution and ACS, should we detect abnormal download volume activity on your account, ACS will automatically suspend access to ACS materials from that suspicious IP. In order to restore access, you will need to provide details of the event and a

American Chemical Society
1155 Sixteenth Street, N.W. Washington, D.C. 20036 pubs.acs.org

remediation plan to prevent future occurrences. For reference, a copy of the required incident report can be found here. We apologize for any inconveniences this may create, but at the present time, this precaution is the most effective way of thwarting additional fraudulent activity.

After consulting with U.S. law enforcement authorities on how best to investigate and prevent these matters, we ask that your institution take every step to preserve any-and-all evidence, in whatever form, relating to illegitimate downloading incidents. Law enforcement advises, in particular, that it is especially important not to "over-write" any potential cyber evidence that your institution's servers may contain. As such, we ask that your institution preserve the log files of any download activity during a known security breach. In particular, please retain the specific IP address, port, timestamp and format (i.e. GMT, UTC, etc.), and originating IP address and logs of the proxy server (if involved) for every ACS download. In addition, we ask that you retain any additional details for each session, such as user agent string and browser type.

We are making every effort to identify the perpetrators and help to prevent future cyber-attacks to our systems and those of our customers. ACS thanks you in advance for your shared commitment to increased network and data security.

If you have any questions about this matter or your account, please contact **acs_pubs_assist@acs.org.**

Sincerely,

Brandon A. Nordin
Senior Vice President
ACS Publications