Report Suspicious Cyber Incidents

SYSTEM FAILURE OR DISRUPTION

Has your system or website's availability been disrupted? Are your employees, customers, suppliers, or partners unable to access your system or website? Has your service been denied to its users?

UNAUTHORIZED CHANGES OR ADDITIONS

Has anyone made unauthorized changes or additions to your system's hardware, firmware, or software characteristics without your IT department's knowledge, instruction, or consent?

SUSPICIOUS QUESTIONING

Are you aware of anyone attempting to gain information in person, by phone, mail, e-mail, etc., regarding the configuration and/or cyber security posture of your website, network, software, or hardware?

SUSPICIOUS E-MAILS

Are you aware of anyone in your organization receiving suspicious e-mails that include unsolicited attachments and/or requests for sensitive personal or organizational information?

UNAUTHORIZED ACCESS

Are you aware of anyone attempting (either failed or successful) to gain unauthorized access to your system or its data?

UNAUTHORIZED USE

Are unauthorized parties using your system for the processing or storage of data? Are former employees, customers, suppliers, or partners still using your system?

We encourage you to report any activities that you feel meet these criteria for an incident. Note that our policy is to keep any information specific to your site and system confidential unless we receive your permission to release that information. US-CERT has partnered with law enforcement agencies such as the U.S. Secret Service and the Federal Bureau of Investigation to investigate cyber incidents and prosecute cyber criminals.

Homeland Security

Report an incident to the
U.S. Computer Emergency Readiness Team

Incident Hotline: 1-888-282-0870

or

www.US-CERT.gov

For more cyber tips, best practices, "how-to" guidance, to sign up for technical and non-technical cyber alerts, and to download this poster, visit www.US-CERT.gov

DHS/PD/OIP/RMD/Feb06/v1.0