Did you encounter suspicious behavior?

Report & Support

1. **See something suspicious?**
   If you receive a potential phishing e-mail, SMS or phone call, receive unexpected requests for password resets or notice general suspicious activity of IT systems, report the cyber incident to qualified personnel.

2. **Report to internal contacts**
   If you are employed by, or working within, an organization with a dedicated IT (security) department, immediately contact them without forwarding any concerning communication.

3. **File a complaint**
   If your organization does not have a dedicated IT security resource, notify the FBI, CISA or the US Secret Service. You do not have to contact all three - filing a report with one is full notification.

---

**How do I prepare in advance of an attack?**

- **Cybersecurity & Infrastructure Security Agency (CISA)** – *Stop Ransomware*
- **US Secret Service Cybercrime Investigations** – *Preparing For a Cyber Incident*
- **National Institute of Standards and Technology (NIST) Computer Security Resource Center** – *Ransomware Protection and Response*
- **FBI** – *Ransomware*
- **US Government Interagency Technical Guidance Document** – *How to Protect Your Networks from Ransomware*

**Who do I contact in case of an attack?**

- You can notify the FBI by filing a complaint at ransomware.ic3.gov. You can also call the FBI's CyWatch 24/7 to report cyber incidents at 1-855-292-3937.
- You can notify the **Cybersecurity & Infrastructure Security Agency (CISA)**. Additionally, you can also report anomalous cyber activity and/or cyber incidents 24/7 to CISA at report@cisa.gov or (888) 282-0870.
- You can notify the local **US Secret Service Cyber Fraud Task Force**.