Enterprise Security and Data Privacy

Boeing's Global Privacy Office is responsible for overseeing the management, use and security of personal information held by the company, including personal data from employees, customers and suppliers. Our privacy program focuses on protecting data, respecting privacy and enabling trust. To safeguard personal information, we employ a principles-based approach to data privacy that aligns with key privacy laws and frameworks in the U.S., European Union and other jurisdictions.

Boeing has also established a Global Security Governance Council to further strengthen governance and enhance coordination of our security activities. Learn more about the work of our council in our Proxy Statement.

Boeing Enterprise Security is critical to Boeing's operations around the world, and we continue to employ industry-leading security practices, while leveraging software and product security engineering to protect our people, property, networks, systems and information from physical and cyber threats. Boeing's security strategy prioritizes detection, analysis and response to known, anticipated or unexpected threats, effective management of security risks and resiliency against incidents. In order to protect both commercial and defense-related businesses and support our production operations, Boeing has adopted security principles that align with global security standards, such as the National Institute of Standards and Technology Cybersecurity Framework, and adheres to contractual and regulatory security requirements.

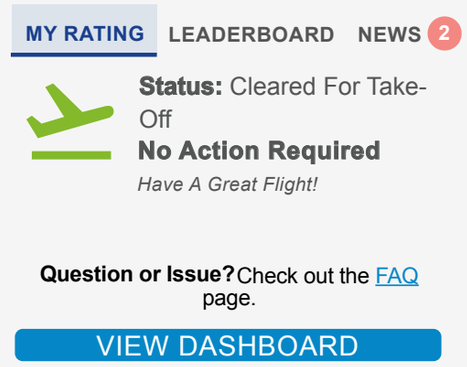
Boeing self-phishing program helps reduce security threats

Boeing Enterprise Security's Self-Phishing Program educates employees about phishing, which involves sending simulated emails to create a "sense-of-urgency" response to click on a link, enter sensitive information, or, best-case scenario, report the "fake" phishing scam.

2022 by the numbers:

- 22% drop in employee clicks on phishing simulations from 2021.
- 17% improvement from 2021 in simulated suspicious email reporting.

It comes down to this: Phishing is the most typical way companies are hacked. It's important for employees to be vigilant against cyberattacks to protect the business and personal data.



Employees get ongoing updates on their phishing results on the company's internal website.

"Phishing is one of the most effective ways threat actors exploit people and companies. It relies on pushing a high volume of phishing-related content and distraction — the worst condition in the modern workplace today. If users aren't careful and trained to spot a phishing email, they may carelessly click on a link or attachment, thus placing Boeing at risk."

Richard Puckett, chief security officer and vice president, Boeing Enterprise Security