CyberSafe at USPS®

Press Play: The Postal Service’s Gamification Approach to Cybersecurity Training
The United States Postal Service (USPS) addresses its cybersecurity risks and challenges through a robust awareness and training program.

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Postal Service Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>The organization is comprised of over 600,000 employees with varying job functions and cyber knowledge.</td>
<td>Raise cybersecurity awareness through ongoing communications, web content, and educational talks across the country.</td>
</tr>
<tr>
<td>Phishing scams are becoming more sophisticated, putting the organization at risk of malware or a data breach.</td>
<td>Provide robust role-based training curriculum on high-priority cyber topics.</td>
</tr>
<tr>
<td>Employees continue to exhibit risky behaviors, including clicking on malicious emails and plugging phones into USPS equipment.</td>
<td>Equip employees to identify and report malicious emails through an anti-phishing program.</td>
</tr>
<tr>
<td></td>
<td>Promote behavioral change through leadership engagement and targeted interventions.</td>
</tr>
</tbody>
</table>

To amplify the impact of its awareness and training program, the Postal Service promotes behavioral and cultural changes through its new immersive learning solution – Cyber Defender.
Cyber Defender allows all levels of Postal Service leadership to assess how employees respond to real-world cyber threats and to analyze behavioral trends that put the organization at risk.

### Benefits of Cyber Defender

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides <strong>custom scenarios</strong></td>
<td>Associates <strong>individual actions</strong> with <strong>organizational impact</strong></td>
</tr>
<tr>
<td>Creates a <strong>hands-on learning environment</strong> and opportunities to apply knowledge</td>
<td><strong>Yields metrics and trends</strong> for measuring <strong>behavior change</strong></td>
</tr>
</tbody>
</table>

**Scenes from the Postal Service's Cyber Defender**
Cyber Defender walks users through ten levels of scenarios dedicated to various aspects of high-priority cybersecurity topics.

**Cyber Defender Components**

- **Ten levels**
- **Six cybersecurity topics**
- **Micro-learning** after each level to reinforce skills
- **Continuous scoring** providing immediate feedback and areas for improvement

**Cybersecurity Topics**

- Workstation Safety
- Social Engineering
- Phishing
- Password Protection
- Malware
- Insider Threat

Cyber Defender utilizes scenarios and micro-learning to emphasize key cyber best practices and give employees the opportunity to practice their skills.
Implementation of Cyber Defender across the organization will yield several long-term impacts.

**Long-Term Impact**

- Organizational cyber behavior change, leading to increased information security vigilance
- Use of analytics and metrics to continuously inform and shape future awareness campaigns
- Increased understanding of how an individuals’ actions can affect the organization

Cyber Defender plays a significant role in promoting and instilling a culture of cybersafety across the entire organization.