expel

CYBERSECURITY AWARENESS MONTH

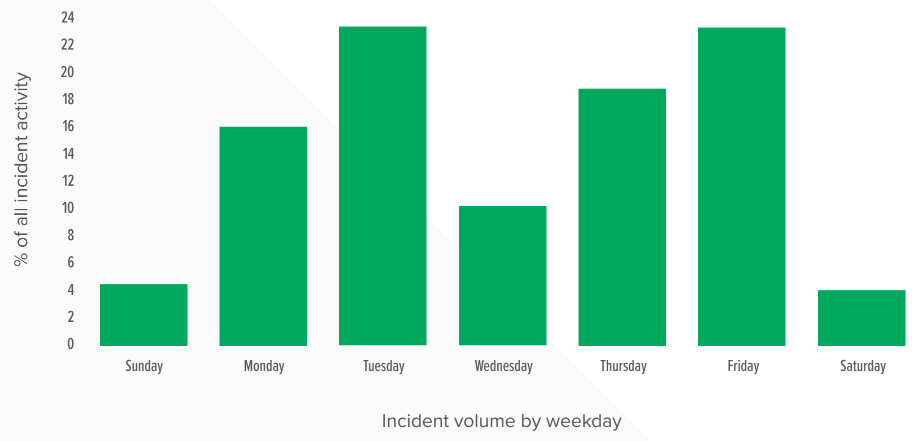
Cybersecurity Awareness Month 2022 presents a great opportunity to reflect on your security team's strategy. Do you have the tools and processes in place to spot and address some of the most common attacks? Expel has compiled recent findings from our security operations center (SOC) to help educate security teams about some of the incidents and trends we're seeing.

Identity is the new endpoint

Identity-based attacks (credential theft, credential abuse, long-term access key theft) **accounted for 56% of all incidents identified by our SOC.**

- **Business email compromise** (BEC) and business application compromise (BAC) access to application data accounted for **51% of all incidents**.
- **Identity-based attacks** in popular cloud environments like **Amazon Web Services (AWS) accounted for 5%**.

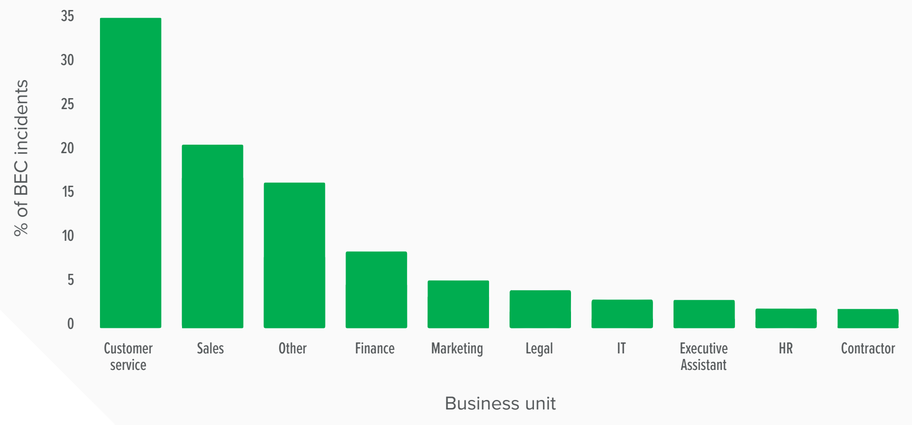
Tuesday and Friday were the busiest days of the week for hackers...



Incident volume by weekday

...accounting for **46% of incident activity volume.** Saturday and Sunday accounted for only 8% of all incident activity volume.

BEC targeting by business unit

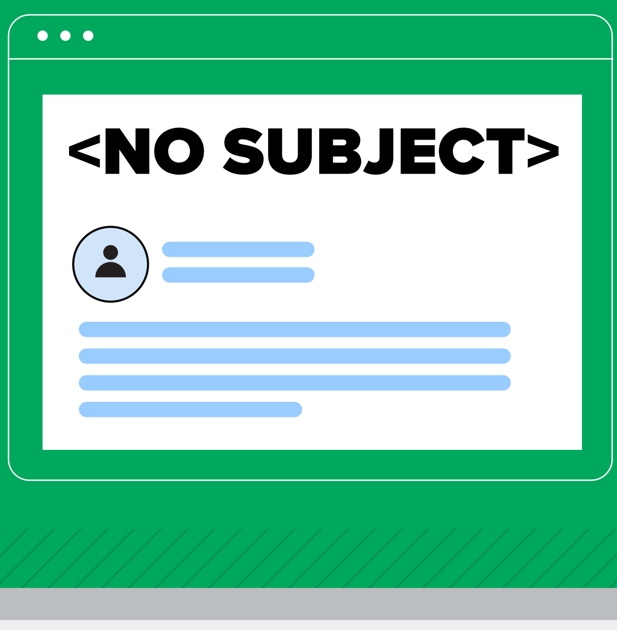


Business unit

Cyber attackers targeted employees working in customer service and sales departments the most, followed by finance, marketing, and legal teams.

Why so much targeting of customer service and sales roles? These roles focus on building relationships *outside* the organization, which means these employees likely open a lot of emails from external senders.

The top subject line for phishing attempts



Cyber attackers have some go-to subject lines for attempted phishing attempts. **The top subject line? No subject line.**

79% of the malicious emails we analyzed left the subject line blank.

Check out our resources at
expel.com/BeCyberSmart

www.expel.com

© 2022 Expel, Inc.