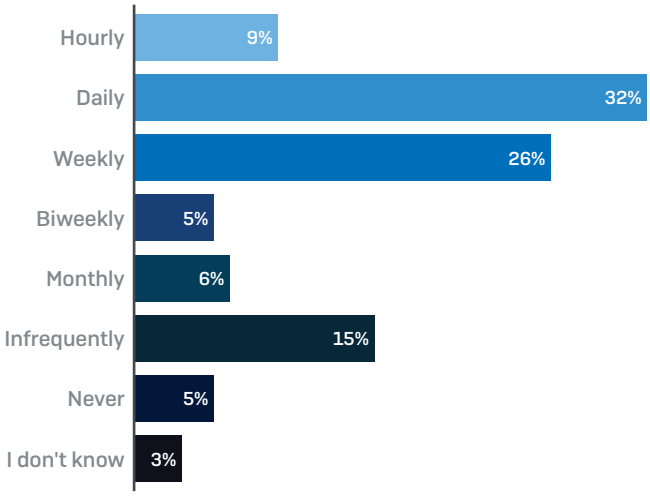
IntegraMSP
PARTNERSHIPS BUILT ON INTEGRITY

The Top Ten Phishing Emails That Hook Us

While big-name ransomware like WannaCry grabs the headlines, phishing is the cybercrime that's consistently hooking organizations week in, week out. In fact, 41% of organizations experience phishing attacks daily or more, and over three-quarters (77%) experience a phishing attack at least once a month*.

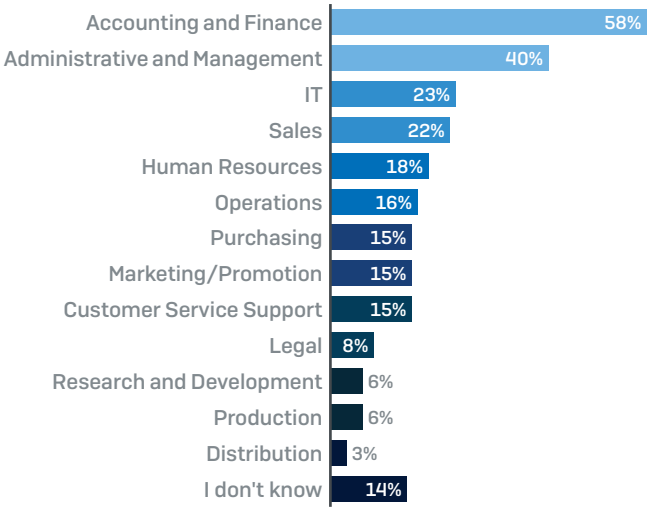
Frequency of phishing attacks



Phishing affects everyone. Organizations of all sizes and all sectors are targets. And cyber criminals are incredibly adept at using social engineering to exploit human weakness. Everyone's on the front line.

Accounting and finance team members are most frequently targeted by attacks – unsurprising, given they have the most direct access to company bank accounts. Cybercriminals also like target those who manage business processes and IT controls, which puts organizations at risk for ransomware and extortion. But cyber criminals don't discriminate. No role is safe from phishing. Anyone who receives emails is at risk.

Departments most targeted by phishing attacks



What is phishing?

Phishing is simply trying to trick people into doing something – that could be opening a malicious email attachment, clicking a link, or transferring funds or confidential data.

Phishing: The Mirror to Our Minds

Today's phishing attacks are highly sophisticated attempts to exploit human nature created by professional cyber criminals. Results from Sophos Phish Threat, a simulation and training tool that teaches people how to spot phishing emails, show that we are most likely to fall emails that focus on:

- **Simple, task-based activities referencing known applications**
  For example, *"[JIRA] A task was assigned to you"*
- **Mundane day-to-day topics**
  For example, *"Let's meet next week"* or *"Car lights left on"*
- **Implication of wrong-doing**
  For example, *"Harassment Awareness Training"*

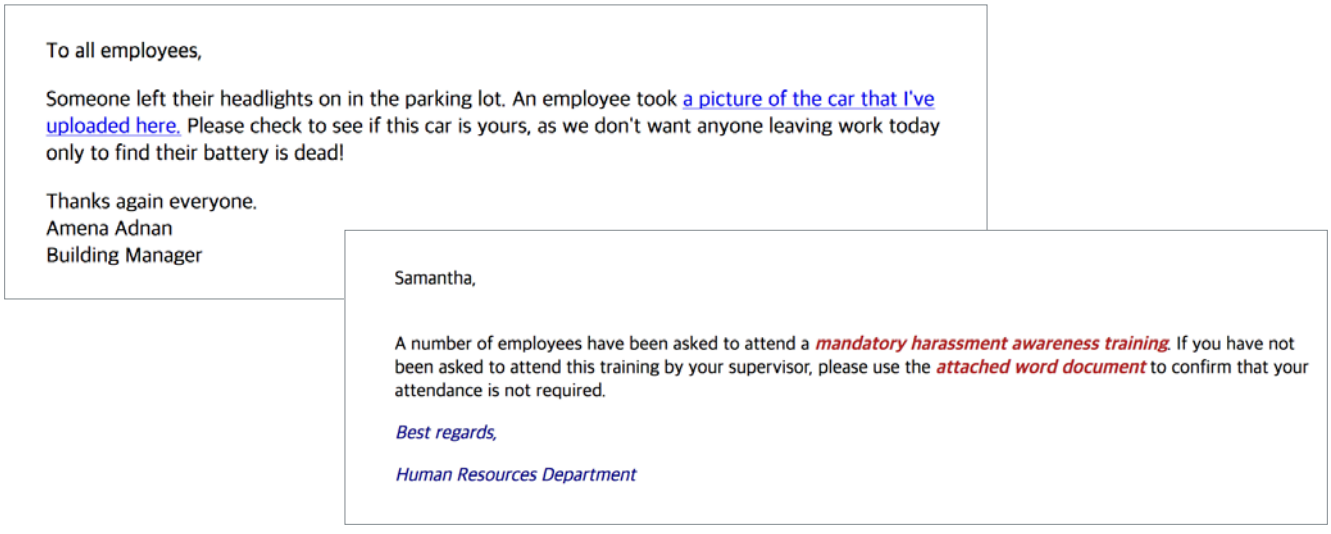
These results reveal a critical point for all organizations: While we're getting wise to fancy visuals and too-good-to-be-true offers, our defenses are down when it comes to everyday work-related emails. Clearly, lack of excitement in an email does not equate to lack of risk.

The important take-away here is that we all need to be on our guard all the time, and even the most mundane looking emails can hide a nasty sting.

Top Ten Emails that People Fall for in Sophos Phish Threat

SUBJECT LINE	CLICK RATE*
[JIRA] A task was assigned to you	38.50%
Let's meet next week	29.10%
Harassment Awareness Training	26.01%
Car lights left on	24.61%
eFax message from {CustomerName} - 2 page(s)	23.55%
Traffic Citation for {EmailFirstName} {EmailLastName}	21.95%
In arrears for driving on toll road	21.36%
Suspicious male spotted outside {CustomerName} Building	20.44%
PLEASE READ - Annual Employee Survey	18.55%
New Email System at {CustomerName} -- Please Read	18.48%

* Percentage of emails that were opened and user clicked on a link



While we're getting wise to fancy visuals and too-good-to-be-true offers, our defenses are down when it comes to everyday work-related emails.

Fighting Back Against Phishing

Phishing often feels like an endless game of cat and mouse between cyber criminals and IT pros, with each side fighting to get ahead of the other. While there's no silver bullet when it comes to phishing, at Sophos we recommend a three-pronged approach to ensure strong anti-phishing defenses.

1. User education and training
2. Pre-delivery: Email gateway
3. Post-delivery: Next-gen endpoint protection

Regular phishing training and education for all staff, using frequently refreshed resources, is the best way to secure your front line against phishing. End users can be any organization's greatest threat vector, but well-trained staff can improve your cybersecurity across the board. We have tools to help educate and test your users through automated attack simulations, quality security awareness training, and actionable reporting metrics. On average, customers see a 31% reduction in phishing susceptibility after just four Phish Threat trainings.

A well-trained staff is an excellent deterrent, but the more phishing emails are blocked at the gateway, the less frequently your users will find real malicious email in their inboxes. We use Sophos, which blocks malicious links, attachments, and phishing imposters before they ever reach end users. Plus it protects employees from fraudulent emails that impersonate trusted senders.

Even the best trained end user can fall prey to human error – especially given how skilled cyber criminals are at impersonating important messages. If this happens, next-gen endpoint protection provides a powerful last line of defense. Powered by deep learning, Sophos Intercept X stops ransomware and other advanced threats from running on your devices even if a user clicks a malicious link or opens an infected attachment.