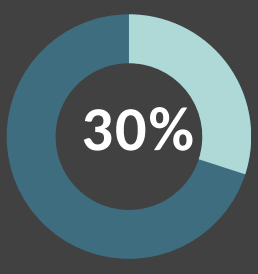
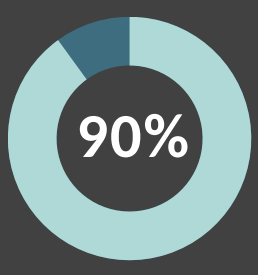
# Gone Phishing

## How to Prevent Your Employees from Taking the Bait

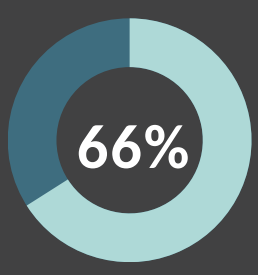
Specially crafted, seemingly legitimate-looking emails used to trick employees into providing confidential data (usernames, passwords, payment card details)



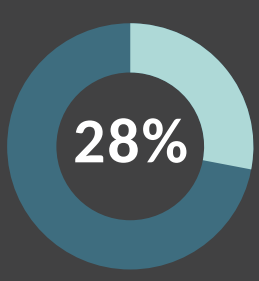

Phishing emails that are opened




Security incidents involving phishing




Malware installed via email attachments




Phishing intended to steal financial data

## Consequences of Phishing

- Malware infections
- Compromised accounts
- Loss of data/money
- Loss of productivity
- Employee disruption

**23.7 days**

Average time to resolve a cyber attack caused by phishing

**$4.65 million**

Annual cost of phishing for average organization

## Easy Targets

Employees are:

- Distracted
- Multi-tasking
- In a rush
- Eager to please

**Questions employees should be asking:**

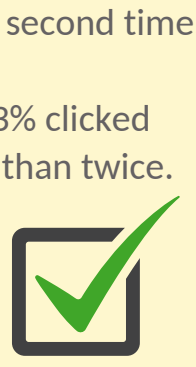

**Only 1 in 5 employees report phishing emails.**

**Fun fact: Employees are more likely to report phishing in the morning and in the middle of the week. "It's Friday...not my problem!"**

## Awareness Works

Preparing users and getting them to think before they click will lower the response rate.

- 15% of users who fell victim once, took the bait a second time.
- Only 3% clicked more than twice.

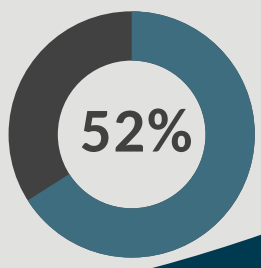


## Phishing Simulations

- Securely test your users
- Identify recipients who click or open
- Provide education
- Reward those that report e-mail to IT

Organizations quantifying a reduction in phishing susceptibility after:

- Phishing simulations
- Awareness training
- Ongoing awareness




CAMPUSGUARD®

To learn more about CampusGuard's phishing simulation testing, contact crm@campusguard.com.