

## Click with Caution:



### Tackling Phishing Threats



62% =

of organizational phishing simulations captured at least one user's credentials.1

of advanced email attacks are being launched from compromised email accounts.2





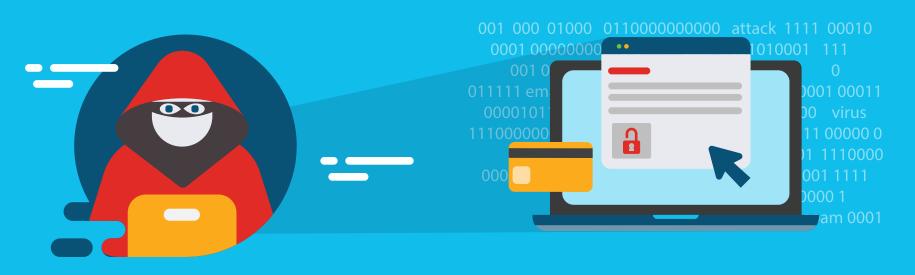
of all attacks on enterprise networks are the result of successful spear phishing.3

<sup>1</sup>According to the The 2018 Duo Trusted Access Report. <sup>2</sup> According to Agari Q2 2019 Email Fraud and Identity Deception Trends. <sup>3</sup> According to the SANS Institute.

95% =



#### Security begins with you



It only takes one wrong click for cyber-criminals to access your company's data



#### Protect you and your family

- Avoid strangers, check name and email address
- Notice mistakes in spelling and grammar

Don't rush, be suspicious of emails marked "urgent"

- Beware of generic greetings, "dear sir/ma'am" Don't be lured by incredible "deals"
- Hover over the link before you click to ensure it has a secure URL (https://)
- Never give out personal or financial information based on an email request

Don't trust links or attachments in unsolicited emails

# users and customers

How Cisco protects its

As a global enterprise, Cisco creates a robust internal education program. Key aspects include:

- Monthly, company-wide educational phishing campaigns that gradually become more complex
- Cisco administrators spear phish high-risk users
- Fooled employees are redirected to an internal education site, the "phishpond"
- Leaders commit to ongoing awareness activities to maintain best practices

**FOR MORE BEST PRACTICES** 

Read our new Email Cybersecurity

**Report** for expert guidance and tips

PEOPLE, PROCESS AND TECHNOLOGY

Learn about technology and resources Cisco recommends to its customers