CISCO

Click with Caution:
Tackling Phishing Threats

62%
of organizational phishing simulations captured at least one user's credentials.[1]

27%
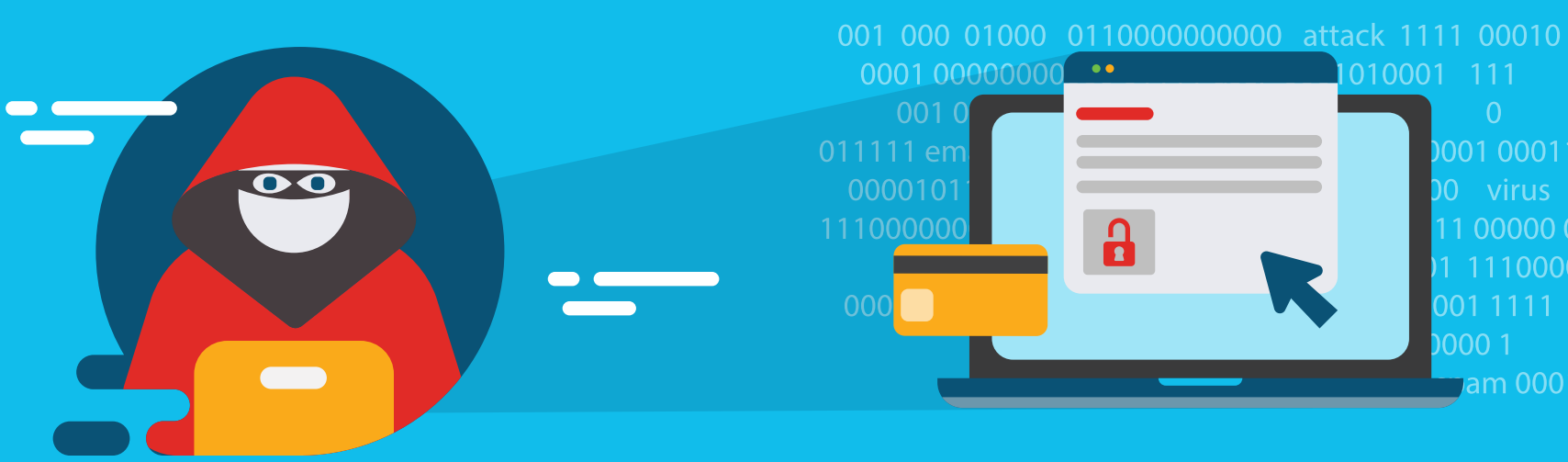of advanced email attacks are being launched from compromised email accounts.[2]

95%
of all attacks on enterprise networks are the result of successful spear phishing.[3]

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

Security begins with you

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

Phishing tips
Protect you and your family

- Avoid strangers, check name and email address
- Don't rush, be suspicious of emails marked "urgent"
- Notice mistakes in spelling and grammar
- 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

How Cisco protects its users and customers

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