SPOTLIGHT ON CYBERSECURITY

Understanding and Defending Against Social Engineering

A Spotlight on How You Can Protect Your Organization from Social Engineering Attacks

StratisAdvisory

RISK | STRATEGY | CYBER COMPLIANCE MANAGEMENT

Recognizing the Types of Social Engineering Attacks

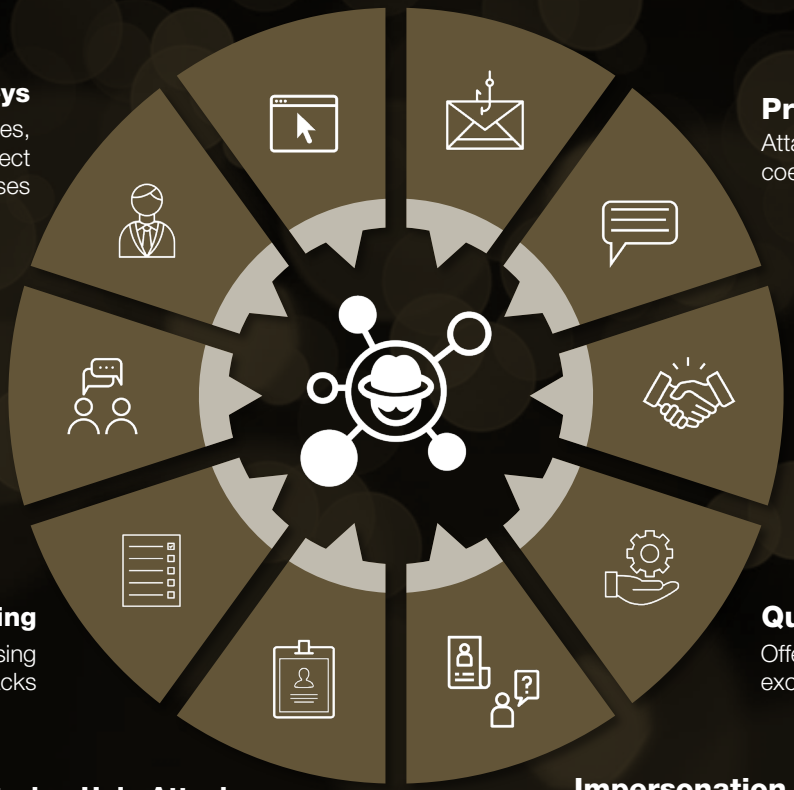
In today's digital age, social engineering poses a significant threat to workplace security. This deceptive practice manipulates human psychology to extract sensitive information or prompt actions that breach security. Social engineers use methods like spear phishing and baiting to access confidential data. It's crucial for organizations to recognize the types of social engineering in workplaces and the emerging threats.

Tailgating (Piggybacking)
Following a person with authorization through entry points to gain unlawful physical access to protected locations

Phishing
Attackers pretend to be reliable sources, usually in emails or messages, to fool victims into disclosing personal information

Quizzes and Surveys
Involve the use of deceptive questionnaires, often shared on social media, to collect personal information for malicious purposes

Pretexting
Attackers manufacture narratives or personas to coerce victims into divulging private information



Reverse Social Engineering
A person-to-person attack where the victim is tricked into divulging private information about themselves or into giving the attacker access to their system or network

Baiting
Luring people in with promises—like free downloads—in an attempt to coerce them into disclosing personal information or downloading malicious software

Whaling
Used to deceive prominent people into disclosing personal information or taking malicious attacks

Quid Pro Quo
Offering a benefit or service in exchange for sensitive information

Watering Hole Attacks
Compromises a trusted website to deliver malware or gather information from the targeted group

Impersonation
Posing as someone else, either in person or virtually, to win someone over and coerce them into disclosing personal information or doing specific tasks

STEPS TO PROTECT YOUR ORGANIZATION

Risk Assessment

Educate Employees

Multi-Factor Authentication

Access Limits

Critical Evaluation

EMERGING CASES OF AI-ASSISTED ATTACKS

In February 2024, a finance worker at a multinational firm was deceived into paying out $25 million to malicious actors using deepfake technology.

The finance worker was invited to a video conference with the Chief Financial Officer (CFO) and other participants.

During the video conference in which the finance worker recognized the other attendees, $25 million was transferred to five (5) bank accounts.

COMMON SCAMMING TACTICS

BRAND IMPERSONATION

Fake websites, emails or logos that resemble legitimate brands to look like official transactions

FEAR OR URGENCY

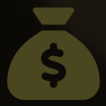
Notifications that will seem to trigger adverse effects when not acted upon immediately (ex. computer virus, credit transactions, copyright violations)

APPEAL TO HELP

Appealing to the person's better nature (ex. a link shared in social media to help a friend fill out surveys, pledges, etc.)

PRETENDING TO BE A PERSON IN AUTHORITY

Messages that claim to come from government agencies, officials, or celebrities



GREED / BIG FORTUNE

Emails that offer big financial rewards in exchange for a small fee

CURIOSITY

Clicking of social media posts that seem to have gone viral

Discover what Stratis Advisory can do for you

Cybersecurity Risk Assessment

Beyond Service and Organization Controls (SOC) audit(s), penetration testing, and PCI Security Standard assessments, dedicated risk assessments help you understand the inherent risks in information technology systems, processes, and programs. Stratis can execute your cybersecurity risk assessment to identify broader risk identification and control mitigation across key information systems.

Cybersecurity Program

Information systems documentation is typically disparate, involves multiple inputs from various third-party vendors performing a specific function, technically focused vs. operational execution, and fragmented without identified ownership across various functions. Stratis can consolidate your information systems and support your chief information security officer (CISO) with developing and maintaining a sustainable enterprise-wide cybersecurity program.

NYS DFS Part 500 Annual Cybersecurity Program Certification of Compliance Readiness

Operating as a New York State Department of Financial Services (NYS DFS) regulated institution such as a bank, insurance company, money transmitter, trust company, etc. (or applying for a license) requires an organization to annually certify to maintaining a compliant cybersecurity program. Stratis can assess the readiness of your organization to submit a certification of compliance prior to the annual April deadline.

Stratis Advisory | 1.415.352.1060 | www.stratisadvisory.com | info@stratisadvisory.com