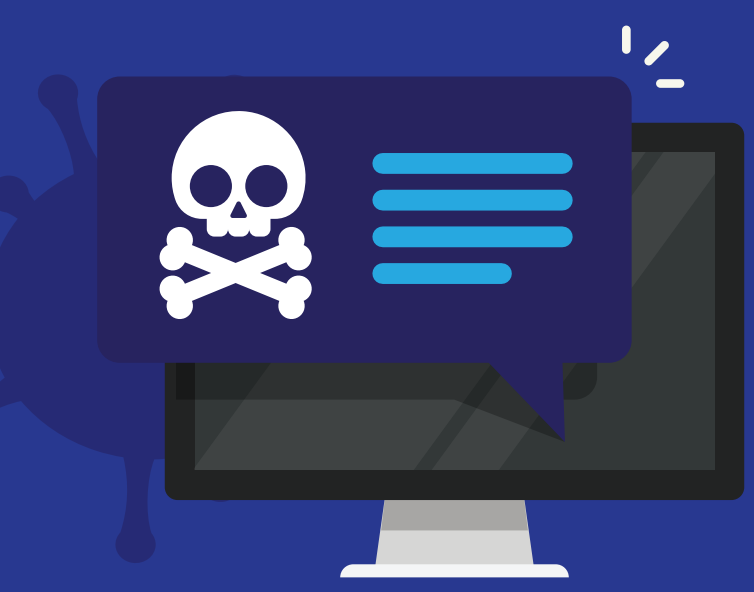
IDENTIFYING & AVOIDING COVID-19 SCAMS

Cyber scams historically rise during national emergencies and the current pandemic is no exception. Protect your data with these best practices to avoid COVID-19 themed attacks.



RED FLAGS

Regardless of the method there are a number of red flags scams share.

- ATTACHMENTS
- HYPERLINKS
- SENSE OF URGENCY
- TYPOS/GRAMMAR
- UNSOLICITED
- UNUSUAL REQUESTS

HOW CAN SCHNEIDER DOWNS HELP?

The Schneider Downs cybersecurity practice consists of experts in multiple technical domains. We offer a comprehensive set of information technology security services including penetration testing, intrusion prevention/detection review, vulnerability assessments, and a robust digital forensics and incident response team.

CONTACT US

WWW.SCHNEIDERDOWNS.COM/CYBERSECURITY

CYBERSECURITY@SCHNEIDERDOWNS.COM.

If you suspect your organization is experiencing a network incident our Incident Response Team is available around the clock at 1-800-993-8937.

BEST PRACTICES

1. AVOID CLICKING ON LINKS OR DOWNLOADING ATTACHMENTS FROM SUSPICIOUS EMAILS
2. DO NOT REPLY TO UNSOLICITED COMMUNICATIONS (EMAILS, TEXTS, CALLS)
3. HOVER OVER LINKS AND HEADER INFORMATION TO SEE FULL URLS AND ADDRESSES
4. NEVER PROVIDE PERSONAL OR FINANCIAL INFORMATION THROUGH EMAIL OR ON SUSPICIOUS WEBSITES
5. ONLY USE VERIFIED WEBSITES SUCH AS WWW.CDC.GOV OR WWW.IRS.GOV FOR COVID-19 INFORMATION

SCHNEIDER DOWNS

Big Thinking. Personal Focus.