Common Types of SOCIAL ENGINEERING SCAMS

Social engineering scams—the manipulation of people into giving up confidential information or carrying out specific actions—are common forms of cyberattack. These scams become especially dangerous as remote work becomes more common. Here are five types of social engineering scams to watch out

PHISHING

What it is—Phishing involves attempting to obtain valuable information by tricking people into visiting a fake website or clicking a link that installs malware. This is typically done via email or text message.

How to stay safe—Beware of messages from unknown sources, and do not click links or visit web pages that you are unfamiliar with.

BAITING

What it is—Baiting describes the offer of a reward for taking a course of action, such as clicking on a link. Baiting can also include leaving a USB containing malicious software in public, hoping someone will find it and plug it into their computer.

How to stay safe—Be wary of offers for free or discounted goods and services from unknown sources. Never insert any unknown USB sticks, discs or other hardware into your computer.

QUID PRO QUO

What it is—Quid pro quo involves a seemingly legitimate exchange wherein the targeted person believes they are receiving a good deal, such as technical service in exchange for login details.

How to stay safe—If a deal from an unknown source seems too good to be true, it probably is. Never give out login or security information to someone you don't know in exchange for anything.

PRETEXTING

What it is—Pretexting is when someone impersonates a known co-worker or authority figure in an attempt to gain access to login information.

How to stay safe—Watch out for unusual email addresses, odd text formatting or suspicious spelling errors from anyone asking for access to valuable information.

KRGinsure

© 2020 Zywave, Inc. All rights reserved.