# Outsmart the Scams

BrainStorm

## How to stay ahead of every type of scam

You might think your IT department has your organization's security covered—after all, they're the ones securing servers, code, and sensitive data. But attackers know the real target isn't our technology: it's your user base. Modern scammers use human psychology against us, preying on our fear and impersonating the people we trust. Users are frequently fooled by predators impersonating Microsoft, Google, and even your own IT department.

Read on to learn how to stay a step ahead of the most common security scams.

# Phishing

Phishing scams rely on a combination of trust and fear. A fraudster will impersonate a reputable source and attempt to get you to reveal sensitive information.

***Check your sources***—Always confirm that email addresses are legitimate. Don't download attachments unless they've come from a trusted source.

***Think before you click***—Hover over links to ensure they'll lead where the email tells you they'll lead.

# Malware

Malware is any type of software that's intentionally designed to cause damage. Attackers hide malware in document types we frequently use, like .zip files, Word documents, PowerPoint presentations, and Excel worksheets.

***Update, update, update***—Make sure your software is always up to date.

***Educate yourself***—Stay current on the latest scams—never assume you're too smart to fall for one.

# Ransomware

Ransomware is a specific type of malware that holds your files hostage and demands a monetary payment to get them back. Depending on the complexity of the ransomware, it can do anything from encrypting your files to locking an entire hard drive.

***Don't pay the ransom***—Paying the ransom isn't a guarantee that you'll get your files back. Alert IT immediately.

***Create secure backups***—Always make sure you have an alternate way to access your files.

# IT Support

The telephone technical support scam can be the most difficult to spot since it can be hard to distinguish from legitimate tech support calls. A scammer will call a user claiming to work for the support desk, hoping a user will divulge passwords, personal information, or even money in exchange for help.

***Hang up***—Hang up and call the support desk using the number your employer provides. The help desk will verify whether or not the call you received was legitimate.

***Know what a phone scam sounds like***—Check out this ***short video*** to see how scammers impersonate someone from your IT department.