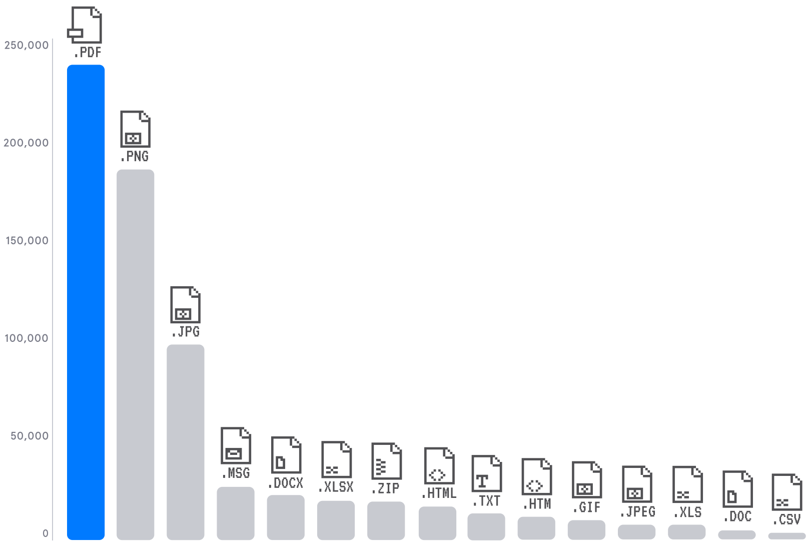
TESSIAN

CYBERSECURITY AWARENESS MONTH

Don't Click That!

While most malicious emails don't actually contain attachments, it's important employees know which file extension types to be most wary of, and how to "test" if an attachment is safe or not.

TOP 15 FILE EXTENSIONS SEEN IN MALICIOUS EMAILS



.PDF files are the clear favorite.

The format is versatile, and can be used to create and run JavaScript files, hide phishing links that can be used to steal a user's login credentials, or deliver information or instructions (like bank details)

* Tessian customers will be alerted when a malicious attachment is detected and can automatically block them

How to identify if an attachment is safe:

CHECK BODY COPY

Even if the sender's email address checks out, you should review the email itself. Is a "customer" addressing by your full name instead of your nickname as he or she normally would? Is a shipping company claiming that you've missed a delivery when you weren't expecting a package? Is your boss acting out of character and urging you to change an account number without following the standard process? Trust your gut!

CHECK THE FILE NAME

Filenames composed of random strings of characters should be a red flag. People (especially in professional settings) don't often save documents with a 20-character alphanumeric code as its name. Similarly baiting titles like "freemoney" or "greatopportunity" should set off your internal alarm bells.

CHECK THE SENDER

Do you trust this person? Have you confirmed that the email address is legitimate? Have you corresponded with them before?

CHECK WITH YOUR SECURITY TEAM

If in doubt, don't open the attachment and let your security team know. Better safe than sorry.

Learn about Human Layer Security.

Want to learn more about how Tessian prevents spear phishing, business email compromise, account takeover, and other targeted email attacks?

GET WEEKLY UPDATES →

REQUEST A DEMO →

TESSIAN

Human Layer Security

TESSIAN.COM

Tessian's mission is to secure the human layer. Using machine learning technology, Tessian automatically stops data breaches and security threats caused by human error – like data exfiltration, accidental data loss, business email compromise and phishing attacks – with minimal disruption to employees' workflow. As a result, employees are empowered to do their best work, without security getting in their way. Founded in 2013, Tessian is backed by renowned investors like Sequoia, Accel, March Capital, and Balderton.