west
‹protect℠

# SAFE Tipsheet

## Password-Protected Zip Files? Look out!

November 2020

We all know that phishing emails are one of the most common online threats and one we should be especially wary of when they contain links to click or attachments to open. We know that we need to make sure we know where they are coming from and that they are safe.

Some attachments may give us a sense of security that they must be safe (like encrypted password protected files), but encrypted archive files (such as ZIP, RAR, and 7Z) that require a password to open to extract the files are actually the most dangerous. **These files get past your anti-virus scanning tools when they come in because without the password, the software can't see what the files contain, so they can't be scanned or flagged as malware.** This makes these files an excellent way for cybercriminals to hide their malware.

Additionally, what makes this more confusing is that we are told that encrypted files are the best way to send sensitive data to someone. So what do we do? We need to stay vigilant, exercise good judgment when receiving and evaluating an incoming email, and be suspicious of those with password-protected files **that you are not expecting** - especially zip files that could be hiding something. Always call and verify the email and attachment on a known good number before opening. WESTprotect customers can simply forward suspicious emails for evaluation.

**According to analysis, how many malicious emails have a .DOC, .XLS, .PDF, .ZIP, or .7Z attached?**

**85%**

SAFE: Security Awareness For Everyone

https://westprotect.com/

WEST, a Williston Financial Group company