Terms & Phrases Likely to be Flagged for Suspicion of Fraud

In the deluge of internal and external communications generated by employees in your organization each day, it can be difficult to spot fraud through monitoring and supervision, unless you know what to look for. Below is a list of keywords — compiled from multiple organizations currently utilizing the Smarsh Archiving Platform — most likely to be flagged for suspicion of fraud. We've also included hypothetical examples of how these terms and phrases might be used to give you a bit of context behind each.

SUSPICIOUS EMAIL TERMS

"Send to my Gmail"

"I like the look of this offer but don't want to discuss details through this account. Send to my Gmail and we'll talk more."

"Don't leave a trail"

"I can help with those transactions, but don't leave a trail. I don't want my name out there."

"Call My Cell/Mobile"

"I've got a deal you're going to love. Call my cell to discuss!"

"Friendly payments"

"As long as you're willing to make a few friendly payments, I think I could make that happen"

"Don't text me"

"Let's discuss further, but don't text me. Call me at home."

"Let's take this offline"

"I've got the facts and figures lined up, let's take this offline."

"TYOP"
(tell you on the phone)

"I've got good news about that deal we discussed! TYOP."

"LDL"
(Let's Discuss Later)

"I've done some research on a few plans and I believe I can help you. LDL"

"Message me on Facebook/Twitter/LinkedIn"

"I've got a few deals with tremendous ROI that may interest you! Message me on Facebook for details."

SUSPICIOUS TERMS FOR SOCIAL MEDIA AND TEXT MESSAGES

"Cook me up"
"Can you cook me up documents that make this situation look better?"

"Money was/is illegal"
"Take proper precautions, the money is illegal."

"Material, non-public information"
"Material, non-public information — DO NOT SHARE!"

"Blame freelancers"
"I'm not worried. If it comes back to us, we can just blame freelancers."

"Expected to announce"
"We're expected to announce the merger later today."

"Leak"
"If there's a leak and the media gets a hold of this, we're finished."

"Do not share"
"For your eyes only. DO NOT SHARE!"

"Shares will be downgraded"
"You didn't hear this from me, but shares will be downgraded Tuesday."

"Deserve to get paid"
"After everything I've done for this firm, I deserve to get paid."

"Top secret"
"DO NOT pass this information around. It is TOP SECRET!"

"Breach"
"There's been a breach, but nobody knows about it yet."

In all but the smallest organizations, manually reviewing content and searching for these terms would be impossible. Fortunately, with the Archiving Platform from Smarsh, you can capture every message and attachment sent by your organization and preserve them in a central archive alongside all communications channels for highly effective monitoring and supervision. With automated capture and management of email, social, text, and instant messages, administrators can create policies that scan for keywords, phrases, or rule violations established by your industry and/or corporate policy, so non-compliant messages can be flagged, reviewed and addressed accordingly.

For more terms and keywords you should be looking out for, read our recent blog posts:

https://www.smarsh.com/blog/terms-phrases-likely-suggest-corporate-fraud-part-1-email/

https://www.smarsh.com/blog/terms-phrases-likely-suggest-corporate-fraud-part-2-social-media-text-messages/

And for direct access to our frequently-updated repository of corporate fraud red flags, visit Smarsh Central:

https://central.smarsh.com/s/article/What-Are-the-Most-Common-or-Popular-Keywords-Phrases-and-Exclusions

smarsh
Capture. Reveal. Respond.