Employers can predict rogue behaviour using your emails

February 18 2014, by Paul Taylor

Something fishy going on in the next cubicle? Check your inbox for clues. Credit: Mark Drago

Most office workers send dozens of electronic communications to colleagues in any given working day, through email, instant messaging and intranet systems. So many in fact that you might not notice subtle changes in the language your fellow employees use.

Instead of ending their email with "see ya!", they might suddenly offer you "kind regards". Instead of talking about "us", they might refer to themselves more. Would you pick up on it if they did?

These changes are important and could hint at a disgruntled employee about to go rogue. Our findings demonstrate how language may provide an indirect way of identifying employees who are undertaking an insider attack.

My team has tested whether it's possible to detect insider threats within a company just by looking at how employees communicate with each other. If a person is planning to act maliciously to damage their employer or sneak out commercially sensitive material, the way they interact with their co-workers changes.

We discovered this by running day-long simulations of an organisational environment in which we monitored multiple aspects of worker behaviour. We looked at the documents the workers used, who they interacted with and their email content. At the beginning of the day everybody was a co-worker. At the morning coffee break, however, we offered a few people £50 to sneak some information out of the system for us. We then continued to offer bigger incentives for more information as the day went on.

Once they agreed to be an insider, workers showed distinct changes in their email behaviour. They used singular rather than plural pronouns, reflecting a greater focus inwards on themselves. They also showed greater negative affect, as their negativity toward the organisation and its representatives leaked into their outward presentation. Finally, their language became more nuanced and error-prone, reflecting the cognitive impact of having to juggle the double identity of being a colleague and an insider.

There was also an important change at the interpersonal level. While other workers continued to show the degree of language mimicry typical of cooperative interaction, the insiders reduced their mimicry of other workers. This change in behaviour, which is suggestive of inadvertent social distancing, increased over time to a point where it was possible to use this metric to differentiate 92.6% of insiders from their co-workers.

Self-protection

Your linguistic footprint might make you easier to spot when you are doing wrong, but it also opens avenues for protecting yourself against crime. The field of authorship attribution looks to identify a person's linguistic fingerprint so that they can be identified as authors of pieces of text. That means you can identify a person even if they use multiple identities online.

This comes in handy in cases such as when you want to try to identify an adult pretending to be a child in a chatroom. The way adults communicate is fundamentally different from the way teenagers address each other and even an adult trying to pose as a child allows some of his or her adult tendencies to seep through. They might overuse a "txt speak", but this style is not as ubiquitous in child's writing as adults expect. Their overuse gives them away.

Once identified, these distinctions can be used to drive an early warning system that either alerts the children to the presence of an adult or acts discretely by alerting the police.

Even in every day scenarios, the traits that give away our bad behaviour can also be used to protect us. When industry worries about cybersecurity, users – the actual customers – are seen as the thorn in the system. They leave passwords under mouse mats, click links that are quite clearly spam and use Facebook as though only nice people will

look at the content.

They are the reason why our technology fails, the cross that the industry must bear. We have to build bigger and better systems so that the irritating, error-prone human can be managed.

Although there are elements of truth in all that, it might be more useful to see humans as an asset. Some of the best security systems are the ones that make the most of the unique characteristics that make us human.

Online banking systems already take advantage of human associative memory – the idea that places, sights, smells and experiences are linked for us in ways that cannot be guessed using an algorithm. In these systems, rather than ask you to present a password, the bank might show you a picture and ask you to recall an associated memory. This is just one way that human memory affords an opportunity for good cybersecurity that other approaches can't beat.

Psychologists have learned to tell quite a lot from user behaviour online and in the workplace. Language use can reveal psychologically important things about who you are and how you are, for example. It can provide clues about your personality, your emotional state, the clarity of your thoughts and the extent to which you are focused on the past, the present or the future.

These all build up to produce a complex picture of the user that could be used as a protective shield. As we try to cope with the myriad cybersecurity threats that affect us daily, this might be the only cast iron technique to ward off those who want to imitate us online for criminal gain.

Human users are imperfect creatures and we have long been exploited for our weaknesses online. But we should also be looking at the problem

from the other side. We should use our human qualities to make better decisions about cybersecurity instead of just beating ourselves up over our inability to remember passwords.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Provided by The Conversation