

# THE EMOTIONS OF CYBER ATTACKS

## When Emotion Takes Over, We Click on the Link

You've found yourself clicking on a link in an email you weren't expecting and as you've done that you realise, wait, what is this email and who sent it? You get that sinking feeling that you've been caught.

You think to yourself: how did I get tricked?

The threat of phishing has been well documented and known for years, but this is still one of the most successful ways for hackers to gain access to our data. So, we are asking the question why? Why does this tactic still work?

**DID YOU KNOW?**
**South Africa has the third highest amount of cybercrime victims globally.**

### STRESS

You're behind schedule or desperately trying to get out of the office. You're going fast and not paying attention. The faster you go, the more likely you are to run into trouble. **Slow down and focus**. Speeding through your email is not worth the consequences of the email breach you're about to cause by clicking on a malicious link.









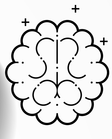

### FEAR

"Do this now or else..." Fear is a powerful stressor and is the most manipulated emotion. The threat of punishment, withholding money or locking your bank accounts are common. So are emails that prey on your fears of forgetting something, fear that you've done something wrong, fear that there's something urgent you're missing. Fear makes us click. **Be brave and vigilant or ask for help.**

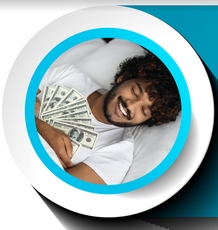
### OVER CONFIDENCE

We can be overly optimistic regarding our abilities to recognise phishing emails. Remember that no matter how computer savvy you are, when someone hijacks your decision-making process then none of that higher brain function is at play. **Don't let your guard down!**









### GREED

To claim your millions, click here! Remember, if it sounds too good to be true, then it probably is. Do not be manipulated by prizes won or unbelievable price drops of items you have been eyeing. **Trust your gut and double check competition winnings.**

### AUTHORITY

People tend to comply with requests from authority figures. Hacker's often use this tactic to ask employees to complete a task, not ask questions, and to do it quickly. The best thing to do in this situation is to **get in contact with the individual who sent the email in another way other than email**. Calling is best, but a quick text is good as well. The pressure from wanting to please your boss might cost you more than you might think.





For all of these emotional situations, it's necessary for us to be mentally present. Understand that hackers are now experts in social engineering. They know what to say to trigger your emotional brain and often use a variety of tactics at once.

### HOW TO PREVENT IT?



- Focus on preventing the phishing aftermath with this 6-second rule:
- **Wait for 6 seconds for the brain chemicals (caused by your emotions which hijack your decision-making process) to diffuse. This means when you read an email that creates a sense of urgency then analyse it BEFORE clicking on ANY link.**
- Remember this: assume that there's something phishy about every link or attachment in every email.
- Pay attention: what is the email trying to get you to do? How is it trying to get you to do it?
- Remember the 6-second rule.

Once the logical side of your brain catches up to your emotional side, you can use logic to explore the email in more depth to see if it is valid.