BALANCING **HUMANS** AND **MACHINES**

Aaron Higbee, Co-founder and CTO, PhishMe, discusses the future of phishing defence and asks which side of the fence the future of defence against phishing attacks lies: human or machine?

Most modern cyber-attacks are ignited with a phishing email. Since the attack vector is digital, we are instinctually inclined to look for a digital solution. After all, computers can run complex algorithms, they don't get tired, and they provide 24/7 support, nearly always at peak performance levels.

Just in the last year, hackers have used them to bring multinational companies to a stuttering halt, derail the most publicised election in the world, and bring entire governments offline for extended periods of time. Moreover, humans are a vulnerable target and gateway to some very advanced digital systems.

Be it through a phishing email or a phone scam during tax season, hackers have mastered the art of social engineering. They know how to bypass our normal caution and get us to act impulsively. Threat actors do this by employing tricks of human psychology, often leveraging emotional triggers of fear, curiosity, emotion and urgency. Or, in some cases, inattention. This is the case with business email attacks carried out early in the day, when employees sip coffee and sleepily dispense with last night's email pile. Attackers also craft seasonal campaigns around tax deadlines and holidays like Christmas. And they elicit stress-based responses whilst tapping into our greed with irresistible promotions or time-sensitive tax-rebates. Add personal information freely available on the dark web (or from a disgruntled employee), and it's not hard to use employees to gain network access.

Humans are a vulnerable target and gateway to some very advanced digital systems.

Given that computational power is always increasing, how can the human compete with it? And if we are, in fact, the weakest link in cybersecurity infrastructure, isn't there an argument to be made for removing the human element from cyber security?

Of course not...

Humans have many advantages over their mechanical and digital co-workers. Even the most enthusiastic robophile will admit there are still some things humans can do to a much higher standard than machines, and key aspects of phishing protection are a good example of this.

Greetings, for example, tend to be good places to catch hackers out. It can be as simple as one of your contacts saying: 'Dear John' instead of the usual brief 'John' that you might be used to. A computer doesn't get the subtleties of these changes, but a person who understands the relationship can be put in a position to see a red flag.

While generally seen as a negative emotion, we have the feeling of suspicion ingrained in us precisely to protect us from being blind-sided by a source we thought we could trust. To truly operationalise employees, companies should see intuition as a resource that can have positive effects when used in the correct environment – a resource that computers do not possess.

Another advantage, for instance, is our penchant for doubt. Computers will run

doi:10.1093/itnow/bwx131 Image: istock.com/muratsenel

the checks administrators set up tirelessly - but will go no further, accepting any peculiarities they haven't unambiguously been instructed to look for. As long as an email comes from a trustworthy source, what does it matter to the computer that the account is '*MichaelBreok@gmail.com*' instead of the usual '*MichaelBroek@gmail.com*'?

Another human component that provides value is unpredictability, or creativity. Many hackers make a living out of breaching secure systems and extorting their cyber victims. So, while the rise of malware-as-a-service business models means that more 'layman' actors are engaged in this cyber security arms race, those designing the malware tend to have very deep understandings of the vulnerability they are attempting to exploit. In other words, they know how a machine will react to certain inputs.

A human provides no similar guarantee. They might fall for a phish, or ignore it. They could report it to the police, or flag it to their security provider. They could even forward the email to an undesired target, or register a malware associated domain and bring the campaign to a halt. All these possible responses mean that cyber criminals engaged in phishing campaigns will often have to limit their 'target audience', and spend time creating protections against certain groups receiving a phish. While this might seem like a relatively insignificant benefit, any barrier to phishing distribution is a positive feature.

Lastly, proponents of using the everyday employee in cyber security point to the 'accuracy paradox'. This paradox states that you can have 99.99 per cent accuracy in your defences, but the remaining 0.01 per cent will often translate into thousands of security alerts. Since IT administrators do not have time to investigate all these alerts, the accuracy paradox necessitates human interaction to help with security. It seems companies can see benefits from involving their employees in cyber security, if these same employees don't act as liabilities. What companies really need are employees conditioned to respond to cyber-attacks - who can respond appropriately almost without thinking, even in stressful situations.

Another way to look at this: the weaknesses of machines are the same as the weaknesses of humans designing them. Humans program and monitor the machines. All security plays out in human terms. Luckily, we have the recipe: practice, practice, practice. It's why drills and simulations are a staple of any military induction program - the only way to overlay best practices on the instincts expressed in emotional situations is to make the best practices instinctual, or part of our muscle memory.

It seems companies can see benefits from involving their employees in cyber security, if these same employees don't act as liabilities.

Surveys show that behavioural conditioning can decrease employees' likelihood of responding to a malicious email by 97 per cent after just four simulations - learning exercises where companies phish their own people. The rationale behind its effectiveness is that it goes beyond making users aware that a threat exists, and forces them to practice responding constantly.

So if the humans can be conditioned, will we ever have an AI-free security environment?

Expecting the next generation of cybersecurity professionals to go back to manual security processes is nothing short of folly. Anti-malware programs, firewalls and spam filters do a relatively decent job of keeping most malware away. Sacrificing these resources would be, at a minimum, inefficient.

A good analogy to make is building a fort: any active fortification worth the name should have big walls on the outside, and a set of strict security measures regulating who should and should not be allowed inside. These policies are a good start. But for a truly secure fort, someone should be hired to make sure no one is climbing over the wall, or pretending to be someone else while entering the gate.

It's also important to make sure the guards receive training - there's no point in spending billions on walls if the guards are giving away the gate keys to strangers. Yet this is essentially what happens when employees click on phishing links, and create the avenue hackers need on to the network.

Man + Machine = Defence in depth

Clearly, employees can be both the strongest and weakest links in your businesses' cyber-security. Certainly, they need all the help they can get from advanced technology - after all, hackers can, and often do, employ automated processes to send thousands of phishing emails every hour.

The trick to combating this automated scourge is to operate at a manageable level of technical security and help humans catch potential threats technology might miss. A recent MIT study conducted by the Computer Science and Artificial Intelligence Laboratory (CSAIL), revealed that the future of cyber-security could be part-human and part-bot, exactly for this reason.

So, if you're suffering from indecision and deciding what side of the human-machine fence you should fall on, the answer is to stay on the fence. From there you can see the reality: both sides of the fence are under constant attack and need strong defences. Those defences, some way, somehow, will always involve a human.