PROFESSOR MONICA WHITTY, *Monash University*
https://research.monash.edu/en/persons/monica-whitty

Professor Monica Whitty is the Head of the Department for Software Systems and Cyber Security, where she holds a Professorship in Human Factors in Cyber Security at Monash University. Monica is an expert in understanding the psychological issues related to cyber security and cyber crimes. She was a member of the Global Futures Communities for Cyber Security for the World Economic Forum. Prof Whitty is the author of five books and over a hundred articles.

TIP 1. CYBERSECURITY TRAINING – WHAT NOT TO DO

There are some very unhelpful advice that organisations say that you ought to avoid. Some classics are: 'Don't click on a suspicious link' (no-one really knows what a suspicious link looks like), 'If it is too good to be true….' (it is never too good to be true (criminals usually gradually up the stakes and so 'too good to be true' is not obvious at the start), 'Don't send money to strangers' (usually the criminal has established a trusting online relationship before they ask for money).

TIP 2. CYBERSECURITY LANGUAGE

It is too often touted that 'humans are the weakest link'. This is very unhelpful language and will not motivate employees to engage in cybersecurity behaviours. Organisations only have problems with security because technology fails them. Avoid blaming the employee (they are victims of the criminals' tricks). Instead, consider that humans are the strongest line of defence.

TIP 3. CYBERSECURITY TRAINING FOR YOUR EMPLOYEES

There is no silver bullet for training and your employees will be at different levels of readiness and ability. Avoid annual online learning materials with multiple choices – they typically don't change behaviour and create a divide between the CISOs (Chief Information Security Officer) group and employees – leaving employees unmotivated and resentful. Do understand your workforce and how different groups learn and create multiple programmes that are engaging and ongoing.

TIP 4. HOW TO PREVENT INSIDER THREAT – TIP 1

Effective vetting. Some insiders seek employment in an organisation with the main intention of stealing (IP/money) or causing harm. Therefore, diligent checks, such as their last place of work, employment history, and previous consultancy work, are essential. Ensure the references are from previous employees and trust references that suggest there may be issues with the potential employee.

TIP 5. HOW TO PREVENT INSIDER THREAT – TIP 2

Notice and act upon problematic behaviour. Some employees may have addiction problems or be associated with unsavoury people (e.g., gangs). These individuals may turn to fraud to support their addictions, or pay off blackmailers. Rather than turn a blind eye (as many organisations do), try to tackle known problematic behaviours (e.g., turning up late, long lunches where the employee slips off to the betting shop etc.). This may be a supportive way to help the employee with their problems or closer monitoring to detect potential insider activity.

TIP 6. HOW TO PREVENT INSIDER THREAT – TIP 3

IP theft typically occurs more gradually than organisations realise. Insiders will often try to find potential buyers of the organisation's IP over extended periods of time and sell off IP to more than one buyer. They often go on trips carrying out presentations to entice potential buys. An insider threat programme needs to consider travel policy and arrangements.

TIP 7. HOW TO DETECT INSIDER THREAT

Although organisations may opt to purchase technical tools that detect insider activity, this kit typically doesn't effectively monitor human factors (e.g., deception cues, change in attitude and behaviour). There are a range of human behaviours you might look out for, including a decrease in organisational commitment, language that regularly states 'I' rather than 'we', star employees that have become less engaging or anger over missing out on a promotion. You might help and support these employees to prevent - or monitor more closely to detect.

TIP 8. HOW TO SPOT MIS/DISINFORMATION

The objective of disinformation is to persuade people into believing a point of view (e.g., that climate change is not real, that vaccinations don't work and cause harm). Often, disinformation combines fiction and nonfiction to appear more realistic and uses heuristics to trick people into believing it is true (e.g., including a person of authority in the narrative, using urgency and scarcity). When presented with new information and before deciding, conduct checks (e.g., read credible sources, check the origin of the source of the material, question the motivations of the sender).

TIP 9. AVOID ROMANCE SCAMS – MEET FTF (FACE TO FACE) ASAP

As the world-leading expert on romance scams I have learned that once potential victims have entered into what they believe to be an authentic relationship it is often too late to try to prevent them from becoming scammed. When dating online, it is essential that daters meet their potential date FTF no longer than 2 weeks from initial contact. If their potential date can't – no matter how reasonable the excuses -- it is likely they are a scammer. Move on before it is too late.

TIP 10. UNDERSTAND CULTURAL DIFFERENCES

Any programme to detect, deter, and prevent cyber threats needs to include a cultural lens. We live in a heterogeneous world that is increasingly embracing diversity. For example, understanding how different groups in societies interact with technology (indigenous groups, the elderly, young people, socio-economic differences, etc.) will help shape programmes tailored to these groups.