Top Tips for Human-Centred Security in the Home Working Environment

Mass remote working brought about by COVID-19 will increase the potential for human error due to a range of factors, including uncertainty, workload and heightened levels of stress. It also provides the opportunity for attackers to successfully manipulate human behaviour to compromise information security.

These ISF tips show how new working arrangements can impact the decision-making capacity of employees and provide guidance on how to manage the corresponding risks.

Download the ISF Briefing Paper, Human-Centred Security, here. ISF Members can find related content on ISF Live.

CHANGES IN HUMAN BEHAVIOUR	HOW TO MANAGE
The emotional reaction to COVID-19 will influence risk perception, causing individuals to lower their vigilance and take unnecessary risks.	Set clear expectations and provide guidelines on how to transfer strong security hygiene from the corporate to the home environment (e.g. secure your devices when not in use).
Scammers will exploit COVID-19, using credible messages that encourage individuals to click on malicious links and open malicious attachments.	Analyse attack methods that take advantage of COVID-19 (e.g. phishing), and make employees aware of how to identify and respond to this threat activity.
Working in isolation without the ease of interacting with peers will influence how security analysts make judgements, causing them to misdiagnose or mismanage potential security incidents.	Schedule regular virtual meetings and conduct scenario planning (for both now and beyond COVID-19) to encourage online collaboration in managing risk.
Individuals under added stress will be forced to make 'good enough' decisions based on available tools, technology and information, which may be limited, incorrect or incomplete.	Provide secure access to credible resources, and take steps to mitigate the spread of misinformation and disinformation.
Mental fatigue will set in as daily routines are turned on their head and life under lockdown takes its toll on families. This will lead to a greater likelihood of accidental errors, resulting in security lapses.	Make allowance for the new environment that employees are working in and its impact on efficiency. Provide necessary office equipment and encourage healthy patterns of behaviour (e.g. regular breaks from the screen).
As organisations rush to implement new or untested technologies to accommodate changing work practices, they may underestimate the intent of malicious actors to take advantage of the situation.	Manage the risk of favouring availability over confidentiality by adopting compensating controls. Refresh and communicate your awareness policies in the specific context of the COVID-19 crisis.

FIND OUT MORE

Discover more useful resources at **www.securityforum.org/covid-19/**

About the ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its members. Find out more at **www.securityforum.org**

Information Security Forum

@SecurityForum

info@securityforum.org

REFERENCE: ISF 20 04 06