Identity security knowledge gaps give cybercriminals an opening
What you don’t know can hack you.

Unmanaged devices are prime targets for identity compromise
If organizations don’t act, BYOD will mean ‘bring your own data breach’.

Respondents trust technology with their security and privacy
We need and trust AI to keep us safe.

The average user is
6-10 times more likely
to fall for an SMS phishing attack than an email-based attachment.

Fragmented identity solutions drive up costs, slow down productivity
You can’t afford bad identity.

More than 2,350 respondents from across more than 90 countries took the RSA ID IQ Quiz.

Responses revealed that:

64% did not select the best privacy technologies for reducing phishing.

63% of respondents didn’t know the identity components needed to move toward zero trust.

55% did not understand the full scope of how identity can improve an organization’s security posture.

64% said they’d trust a computer or password manager with their banking information before their partners, closest friend, or financial advisor.

91% believed that AI can detect suspicious access attempts, identity irregularities.

72% believed that people for whom we account on personal devices access professional resources.

97% of cybersecurity experts believed that threat actors target unmanaged mobile devices.

Nearly three-quarters either didn’t know or significantly undervalued the cost of a password reset.

Each password reset costs upwards of $70, and nearly half of all IT help desk costs.

63% of respondents didn’t know the identity components needed to move toward zero trust.

64% did not select the best practice technologies for reducing phishing.

55% did not understand the full scope of how identity can improve an organization’s security posture.

64% said they’d trust a computer or password manager with their banking information before their partners, closest friend, or financial advisor.

91% believed that AI can detect suspicious access attempts, identity irregularities.

72% believed that people for whom we account on personal devices access professional resources.

97% of cybersecurity experts believed that threat actors target unmanaged mobile devices.

Nearly three-quarters either didn’t know or significantly undervalued the cost of a password reset.

Each password reset costs upwards of $70, and nearly half of all IT help desk costs.

30% were prevented from accessing the systems needed to do their work at least once a week.

Cybersecurity professionals believed that users opened more emails on their phones than on desktops, had more difficulty scrutinizing those emails on mobile devices, used personal devices to access professional resources, and/or that unmanaged devices don’t have the same security capabilities as managed devices.

Zimperium 2023 Global Mobile Threat Report

World Economic Forum

©2023 RSA Security LLC or its affiliates. All rights reserved. RSA and the RSA logo are registered trademarks or trademarks of RSA Security LLC or its affiliates in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. 07/23 Infographic