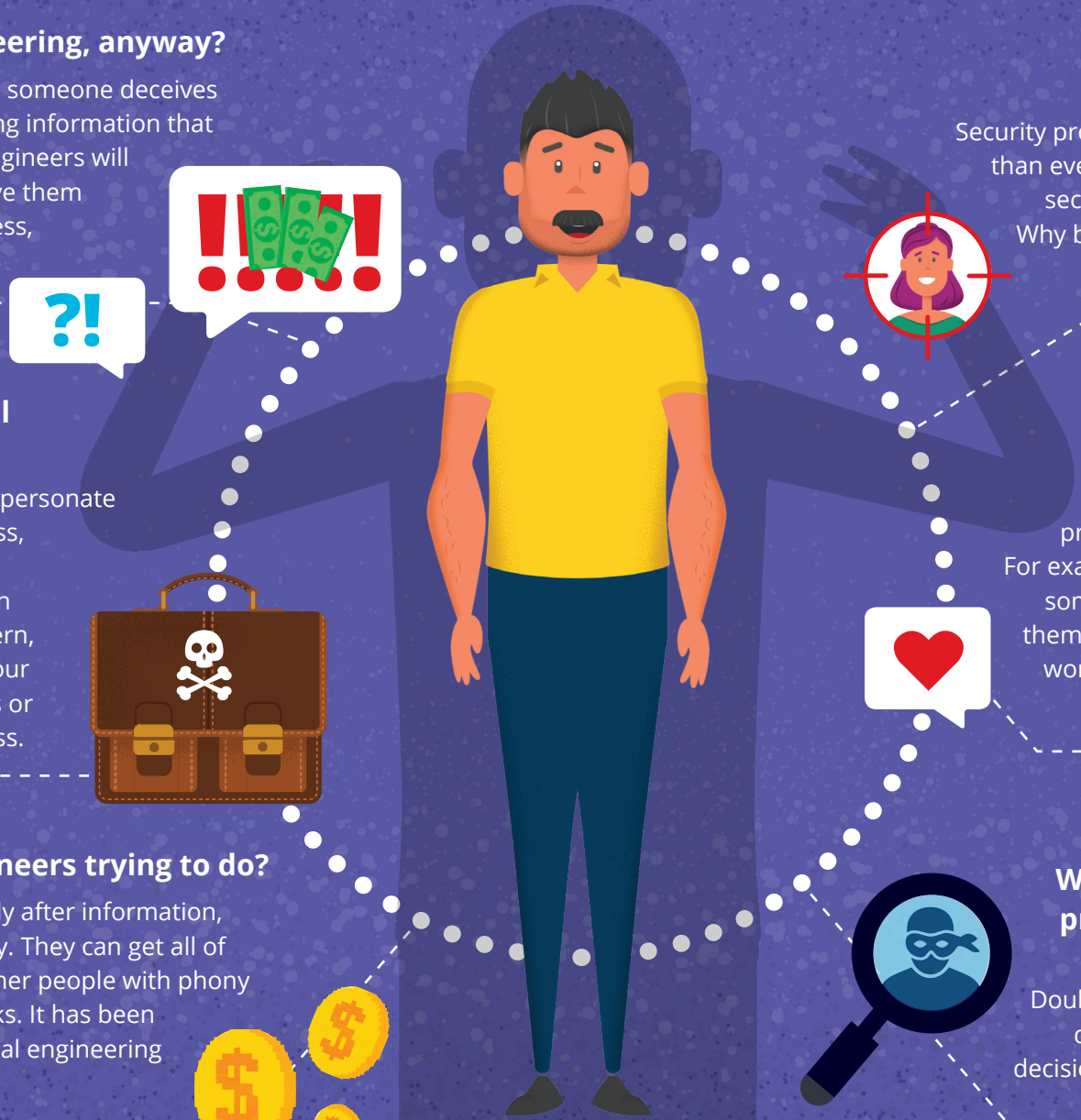
Social engineering

INFOSEC
Office of Information Security

What is social engineering, anyway?

Social engineering is when someone deceives someone else into revealing information that can be exploited. Social engineers will convince their target to give them crucial information or access, or even send money.



Why would someone use social engineering?

Security programs and systems are stronger than ever, but social engineers avoid that security entirely by targeting people. Why break into a system when you can trick someone into letting you in?

How can I spot social engineering?

Social engineers like to impersonate authority figures like a boss, a government agent or a lawyer. Since manipulation is their number one concern, they may also try to get your sympathy with sob stories or pretending to be in distress.

What are some tricks social engineers use?

There are a number of common principles used by social engineers. For example, reciprocity: if they give you something, you're more likely to give them something. Or sympathy: people won't question the story of someone who looks like they're in trouble.

What are social engineers trying to do?

Social engineers are usually after information, privileged access or money. They can get all of these things by tricking other people with phony messages. And yes, it works. It has been estimated that 79% of social engineering attacks are successful.

What's one thing I can do to prevent social engineering?

Slow down the conversation. Double-check everything they say and don't let yourself be hurried into a decision. A lot of social engineer stories can't hold up to close inspection.

Sources: https://datafloq.com/read/social-engineering-attacks-numbers-cost/6068

For any questions, contact the UC Office of Information Security at infosec@ucmail.uc.edu

© 2019 Infosec. All rights reserved.