callsign

HOW IT WORKS

Step-Up authentication

Jamal attempts to access his account using his personal laptop form his home.

His device is free of malware and his keystrokes and mouse movements are consistent with his usual behavior.

Callsign lets Jamal into his account with no friction.

Jamal goes on holiday and attempts to access his account.

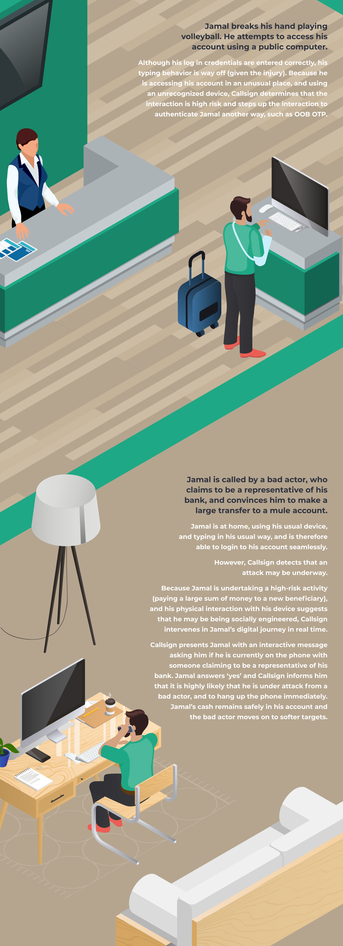
His device is still free of malware and, because he is using his personal device and behaving in a usual way, Callsign recognizes him. However, Callsign has identified that Jamal is in an unusual location. Although Callsign grants Jamal access, it also sends him a push notification informing that a login attempt has been made from a high-risk location. If the login attempt is illegitimate, Jamal is able to inform Callsign and the interaction is terminated.

Jamal is still on holiday. His device runs out of battery, so he attempts to access his account from a public computer.

The public computer he uses is free of malware, but if there were a threat Callsign would deal with it appropriately.

Because the login attempt does not come from Jamal's device, and it is made in an unusual location, Callsign identifies that the interaction is risky. However, Jamal's typing behavior and mouse movements are consistent with his profile, suggesting that the attempt may be legitimate.

Before access is granted Callsign mitigates the risk by sending Jamal a push notification to his mobile device.



Jamal breaks his hand playing volleyball. He attempts to access his account using a public computer.

Although his log in credentials are entered correctly, his typing behavior is way off (given the injury). Because he is accessing his account in an unusual place, and using an unrecognized device, Callsign determines that the interaction is high risk and steps up the interaction to authenticate Jamal another way, such as OOB OTP.

Jamal is called by a bad actor, who claims to be a representative of his bank, and convinces him to make a large transfer to a mule account.

Jamal is at home, using his usual device, and typing in his usual way, and is therefore able to login to his account seamlessly.

However, Callsign detects that an attack may be underway.

Because Jamal is undertaking a high-risk activity (paying a large sum of money to a new beneficiary), and his physical interaction with his device suggests that he may be being socially engineered, Callsign intervenes in Jamal's digital journey in real time.

Callsign presents Jamal with an interactive message asking him if he is currently on the phone with someone claiming to be a representative of his bank. Jamal answers 'yes' and Callsign informs him that it is highly likely that he is under attack from a bad actor, and to hang up the phone immediately. Jamal's cash remains safely in his account and the bad actor moves on to softer targets.