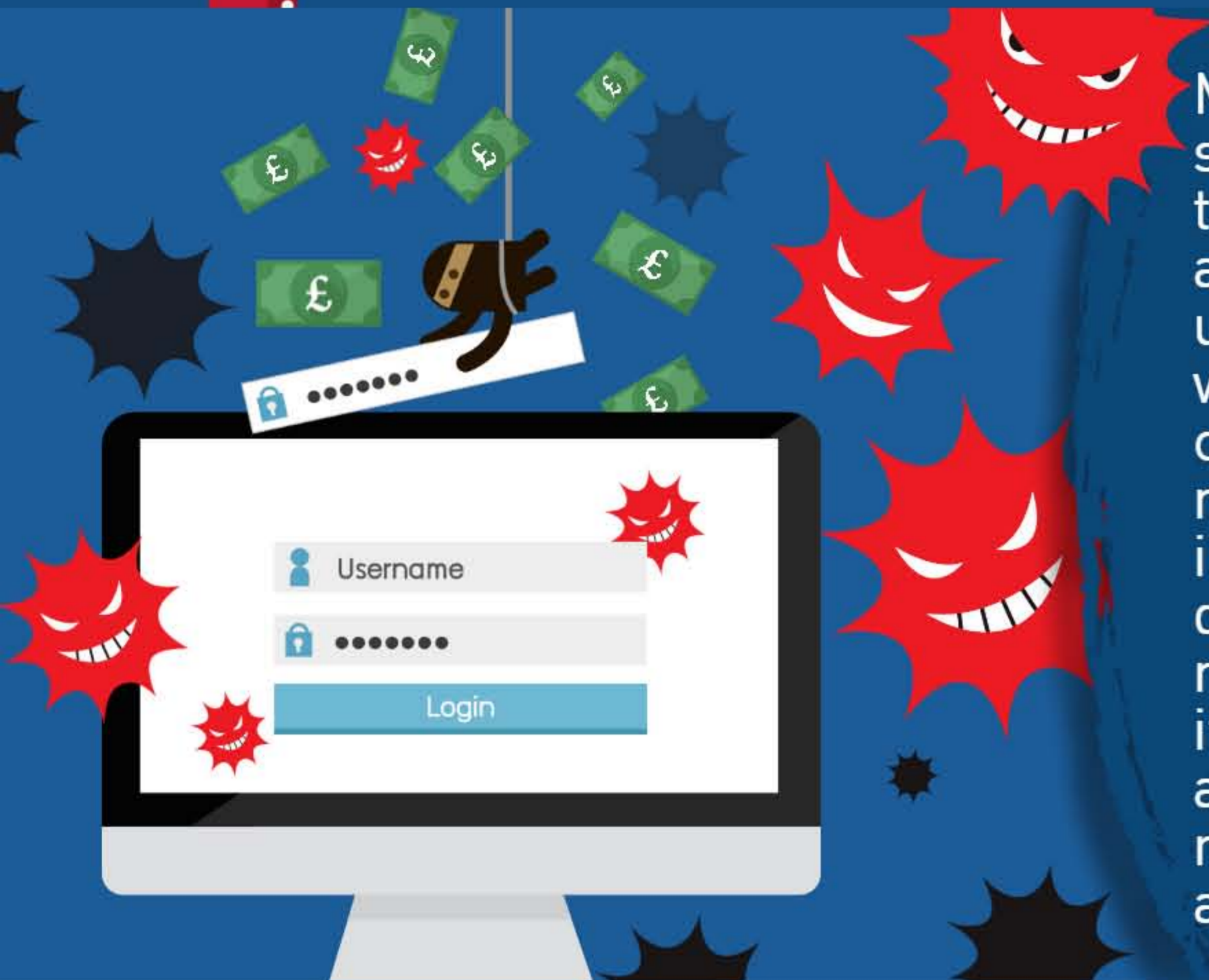


DO YOU REALLY KNOW...



...HOW BANKING MALWARE WORKS?



Malware, which is short for malicious software, refers to any software that's designed to disrupt or damage a system, and cause harm to the user (you). Viruses, trojans and worms are just a few of the most common types of malware. Banking malware is specifically designed to intercept and steal a user's financial details. There are many ways malware can infect a device, whether it be a link to a malicious website in an unsolicited email, text, social media post, or installing an app from an unofficial app store.

> 1.9m

Attempted malware infections that aimed to steal money via online access to bank accounts.

<https://securelist.com>

> 390,000

New malicious software programs detected every single day.

www.av-test.org

£20m

The estimated financial loss to the UK from just one piece of banking malware (Dridex).

National Crime Agency

HOW TO PROTECT YOURSELF...



Don't click on links you receive in unsolicited emails, SMS messages or social media posts. The links may lead to malicious websites, and any attachments could be infected with malware.



Only install apps from official app stores, such as Google's Play Store, or Apple's App Store. Jailbreaking, rooting, or disabling any of the default security features of your mobile device may leave it more susceptible to malware infections.



When logging in to your online banking account, be extremely cautious if you're asked for details such as the 3 digit (CVV) number on the back of your card, the long number on the front of the card, your card's expiry date, or the 4 digit PIN for your card. If the online banking login page you're on does ask for these details, then don't login until you've called your bank to verify that you're logging in to a genuine web page.



Your bank will never ask you to transfer money out of your account and into another. Fraudsters will. If you receive messages, browser pop ups or calls asking you to do this, then don't respond to them. Call your bank immediately.