TOP 7 WEAKNESSES THAT MALWARE EXPLOITS

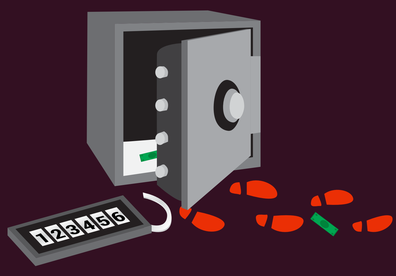
Malware threats are on the rise! So how are these viruses, worms, and trojans continuing to infiltrate businesses around the world?

MOBILE DEVICES

Numerous studies have identified mobile devices as one of the top entry points for hackers. **Symantec** estimates **24,000 malicious mobile apps are blocked each day**. Many mobile apps have insecure data storage which makes them vulnerable to malware. Question mobile apps that ask for access to user data and whether that is really needed.

WEAK PASSWORDS

A Verizon Data Breach Investigations Report found that **81% of hacking-related breaches** leveraged either **stolen and/or weak passwords**. Even more alarming is research by Varonis that found 65% of companies have over 500 users with passwords that never expire. Stay away from birthdates, keyboard patterns, popular phrases (i.e. abc123) and the word password backwards!

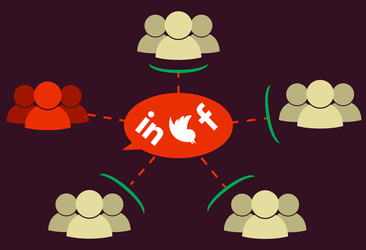


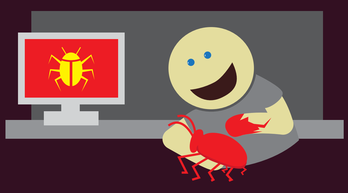
EMAILS AND LINKS/ATTACHMENTS

According to the Verizon Data Breach Investigations Report a staggering **92% of malware is delivered by email.** Cisco found 38% of malicious attachments were disguised as Microsoft Office type files. Resit the urge to click links and open the attachments in emails unless completely confident of the source.

SOCIAL MEDIA

1 in 5 organizations have been infected with malware distributed via social media platforms according to a report from Bromium. James C. Foster, CEO and co-founder, ZeroFOX describes social media as the world's largest attack surface and medium combined. Everything from advertisements to malicious apps to plug-ins to links on social media platforms has the potential to be malware.





CARELESS STAFF

The EY Global Information Security Survey found **34% of organizations see careless/unaware employees as their biggest cybersecurity vulnerability**. In one US State alone the research found 1,464 government officials using "Password123" as their password.

ONLINE ADS (MALVERTISING)

A report from Confiant, an ad security company, found **1 in every 100 ad impressions online have malicious and disruptive intent**. In 2017 Google reported removing 100 bad ads per second. So it isn't just companies selling products buying ad space, attackers are buying ad space on popular websites and loading ads infected with malware.

IOT DEVICES

Research is predicting over 50 billion devices will be connected to the internet by 2020. Symantec found the **top password attackers used to access IoT devices in 2018 was "123456,"** which was used in 25% of all attacks. No password at all, accounted for 17% of the 2018 attacks.