THE 7 MOST INEXCUSABLE MISTAKES

Employee negligence is said to be the most common cause of data breaches in companies according to different studies.

1. TRIVIAL PASSWORDS

23 MILLION OF BREACHED ACCOUNTS IN UK USED EASY-TO-GUESS PASSWORDS SUCH AS 123456

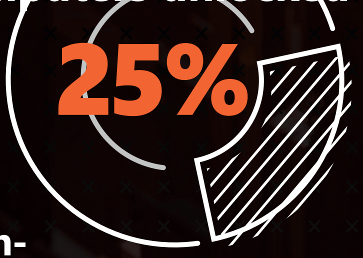
The most common passwords that we see used in corporations are variations of words: Password; Password1; P@ssw0rd; Admin123; strings of numbers or a company name. Even though they meet all the requirements... **they're a definite no-no!**

Source: https://www.bbc.com/news/technology-47974583

2. UNLOCKED COMPUTERS

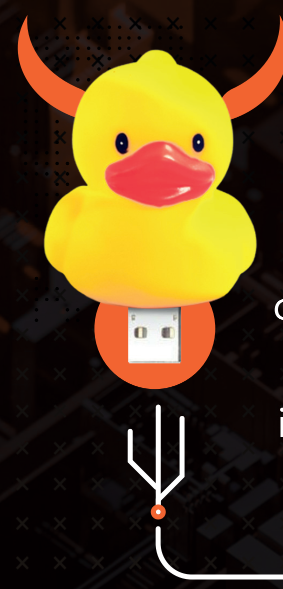
It's terrifying, but more than **25% of United States workers** admit that they leave their **computer unlocked** when they go home at the end of the day! Many users do not lock their computers when they take short trips for coffee. This gives cleaning staff or visitors an excellent opportunity to have a quick peek.

US workers leaving computers unlocked



Source: https://www.shredit.com/getmedia/b5de58fd-7e17-4d18-b718-9eca8d0665a6/Shred-it-2018-North-America-State-of-the-Industry.aspx

3. UNKNOWN (EVIL) USB STICKS AND CABLES

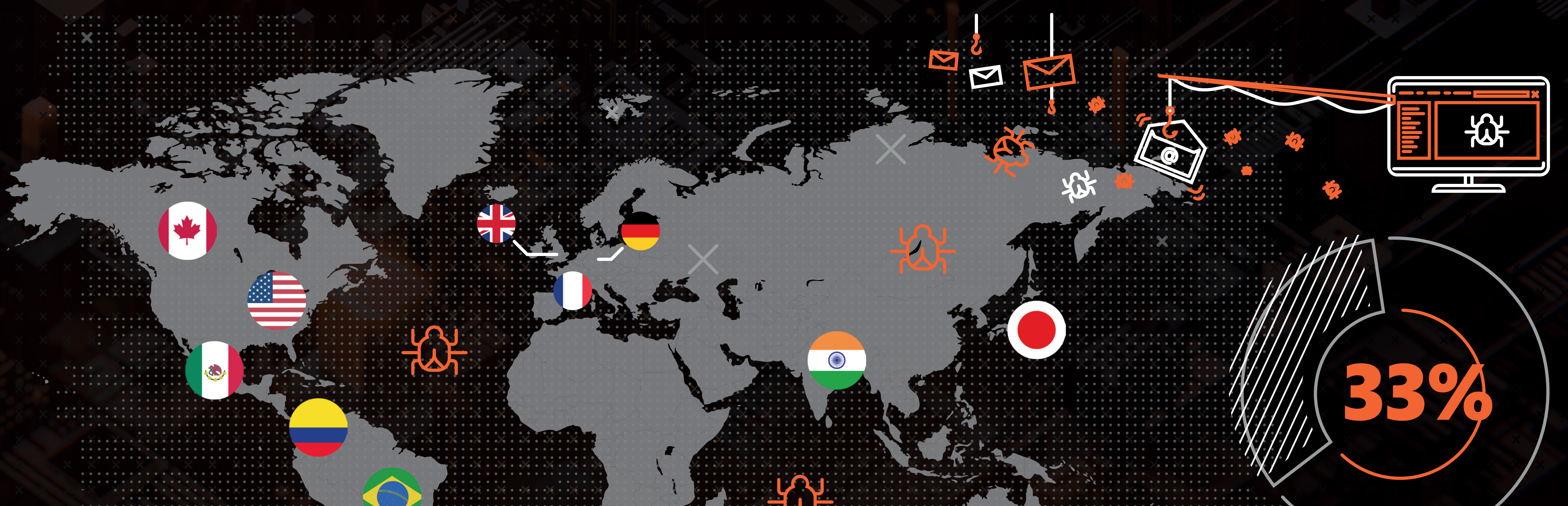


It's fundamental not to plug unknown devices into your computer. Have you heard about **RubberDucky** or **USBNinja**? They enable several attack scenarios, from simple keystroke injection to completely taking over your computer. From there, the tools can be used to execute payloads of any variety.

4. LIKE A 'PHISH' IN A POOL

Phishing emails are one of the most common ways that a hacker can enter an organization. Emails were used in **33% of known, successful attacks on companies across 12 countries**, a study from 2018 shows.

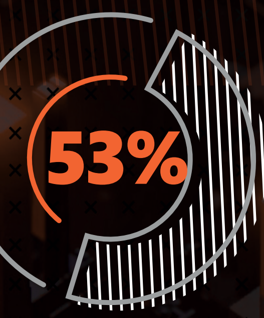
Source: https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf



of attacks made by hackers used e-mail as a way to infiltrate the organization

5. WILD WI-FI NETWORKS

people can't tell the difference between a secured or unsecured public Wi-Fi network.

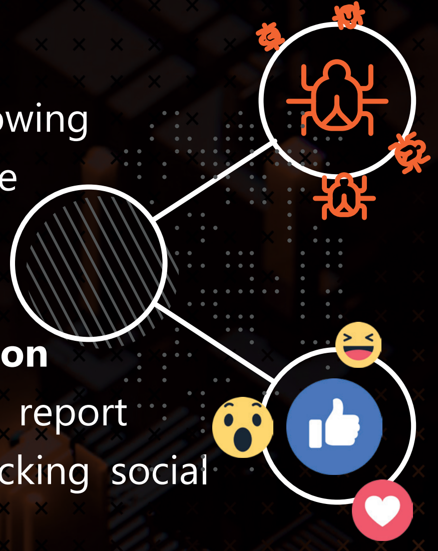


Source: https://www.symantec.com/content/dam/symantec/docs/reports/2017-norton-wifi-risk-report-global-results-summary-en.pdf

It's easy to find open Wi-Fi networks at airports, in restaurants or inside shopping malls. Remember to **connect via VPN** when using not trusted Wi-Fi networks. VPN encrypts your Internet connection to secure it and protects your privacy. **And now the information you send over the network is encrypted.**

6. SOCIAL MEDIA

Downloading untrusted files from social media or following untrusted URLs from your company computer may have the same effect as opening an infected/malicious email attachment. A simple **bot-spam message** on Twitter was able to **grant a hacker access to a Pentagon official's computer**, according to a New York Times report published last year... Do you see the reason for blocking social media at your workplace?



Source: https://www.nytimes.com/2017/05/28/technology/hackers-hide-cyberattacks-in-social-media-posts.html

7. IT'S THE 21ST CENTURY AND YOU'RE STILL NOT USING A PASSWORD MANAGER?

Password managers such as **KeePass** or **LastPass** are an alternative to writing credentials on sticky notes or trying to remember them. We know that users who use passwords managers are more likely not to re-use the same credentials. Why? **Password managers make it easy** to use a different (and random!) password for every account.

CQURE
ACADEMY