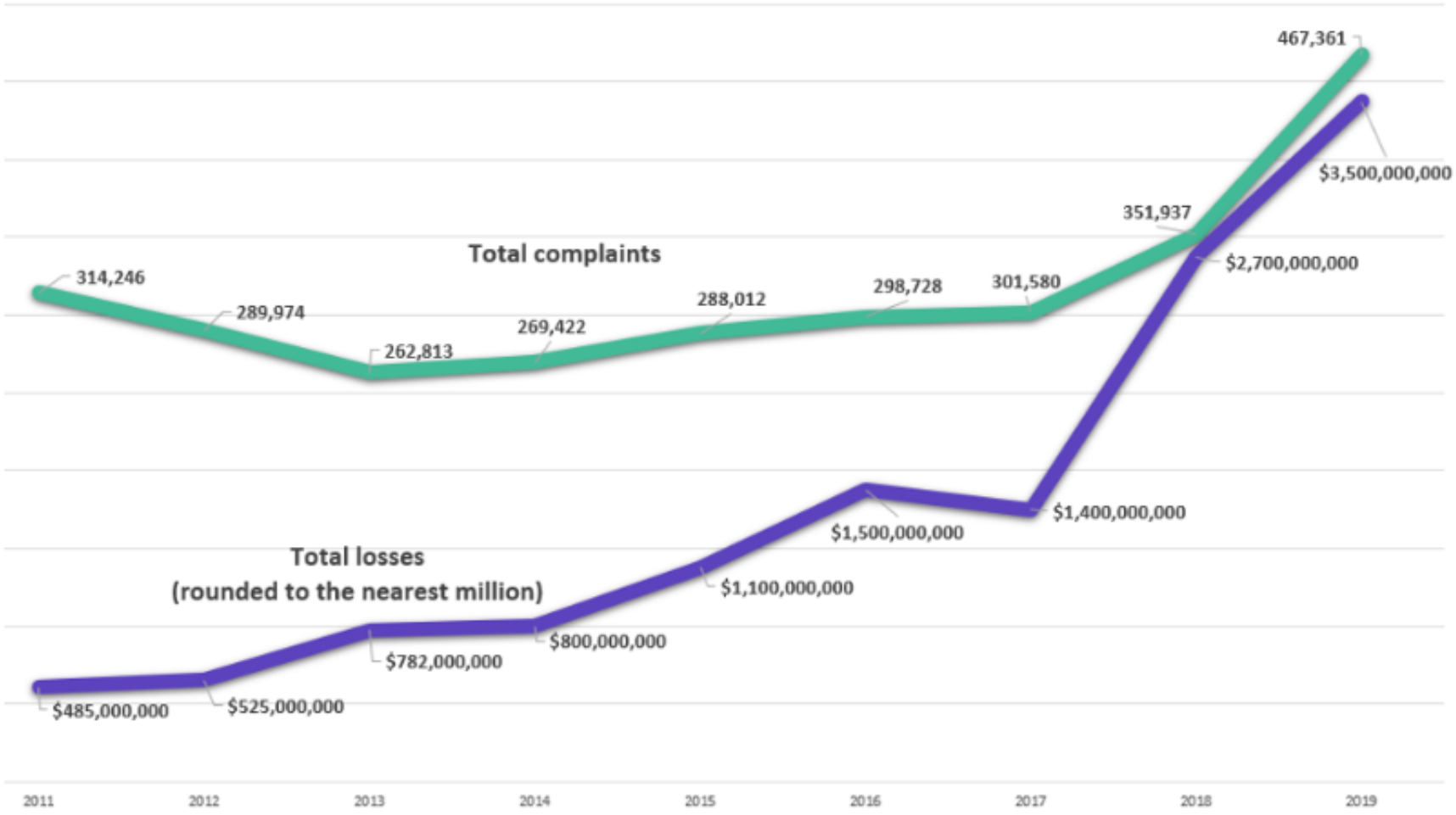
THE BIGGEST DANGER IS YOUR COMPLACENCY

"Success breeds complacency.
Complacency breeds failure.
Only the paranoid survive."

- Andrew Grove, former CEO of Intel



IC3 statistics showing an increase in reports and reported losses since 2011

SOCIAL ENGINEERING – HOW DOES IT WORK?

SOCIAL ENGINEERING IS THE #1 THREAT

Social engineering *is an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.*

OF ALL SECURITY INCIDENTS ARE CAUSED BY YOU!

5 METHODS OF SOCIAL ENGINEERING

- **BAITING**: Baiting is when an attacker leaves a malware-infected physical device, such as a USB flash drive in a place it is sure to be found. The finder then picks up the device and loads it onto his or her computer, unintentionally installing the malware.

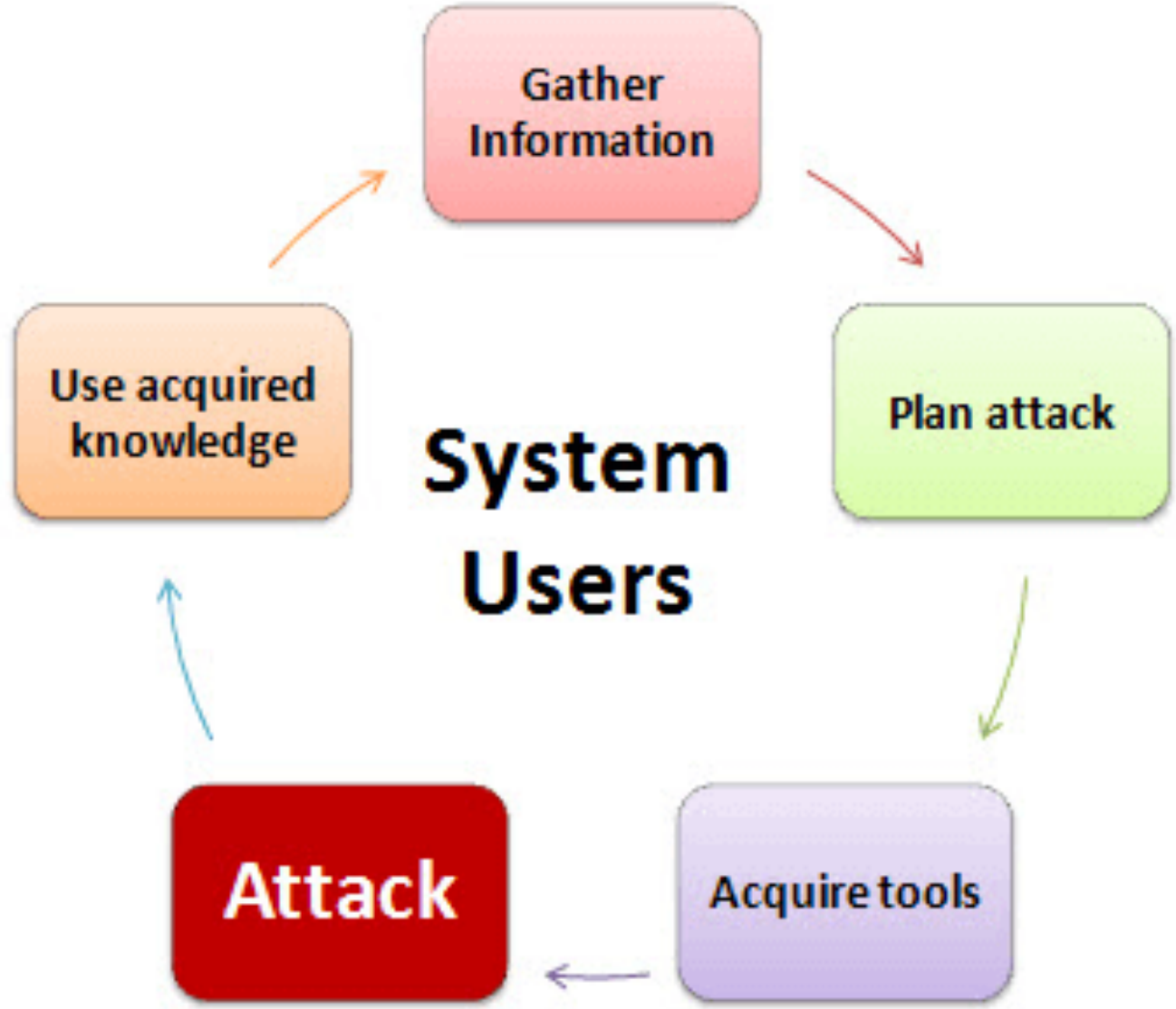
- **PHISHING**: Phishing is when a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source. The message is meant to trick the recipient into sharing personal or financial information or clicking on a link that installs malware.

- **SPEAR PHISHING**: Spear phishing is like phishing, but tailored for a specific individual or organization.

- **PRETEXTING**: Pretexting is when one party lies to another to gain access to privileged data. For example, a pretexting scam could involve an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.

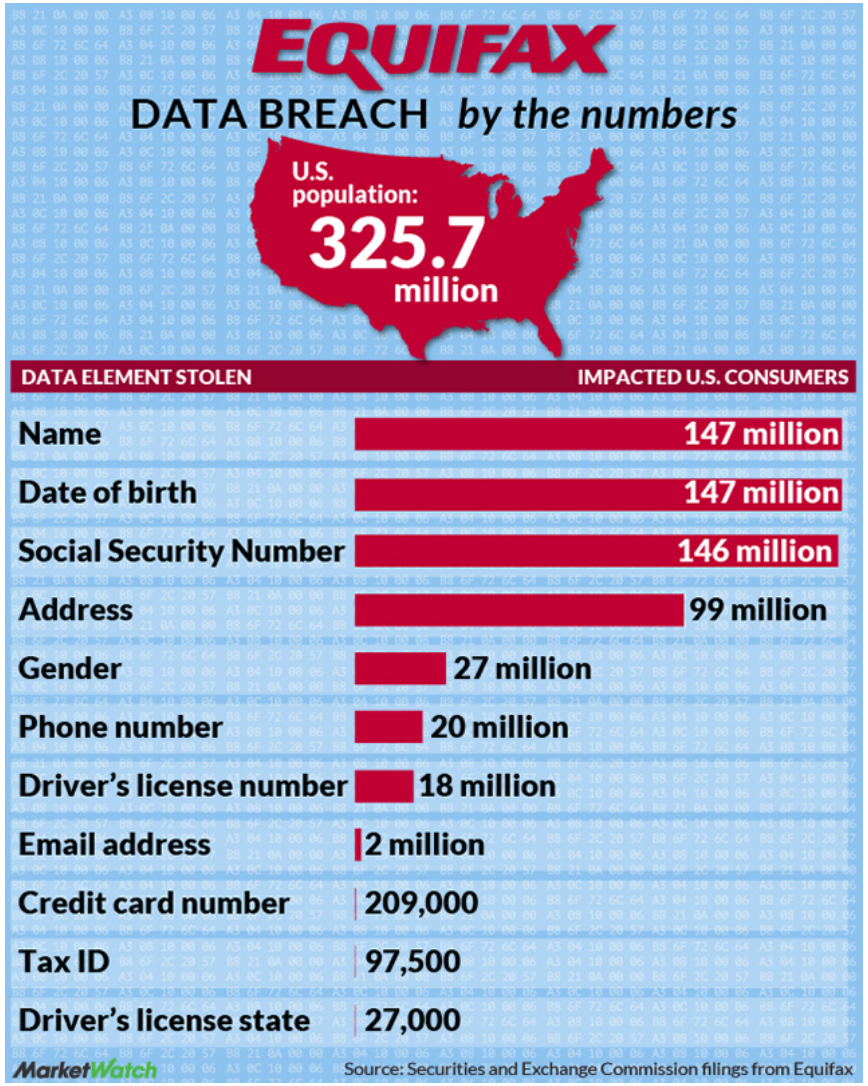
- **SCAREWARE**: Scareware involves tricking the victim into thinking his computer is infected with malware or has inadvertently downloaded illegal content. The attacker then offers the victim a solution that will fix the bogus problem; in reality, the victim is simply tricked into downloading and installing the attacker's malware.

SOCIAL ENGINEERING CYCLE



YOUR INFO USED AGAINST YOU

COMPASS



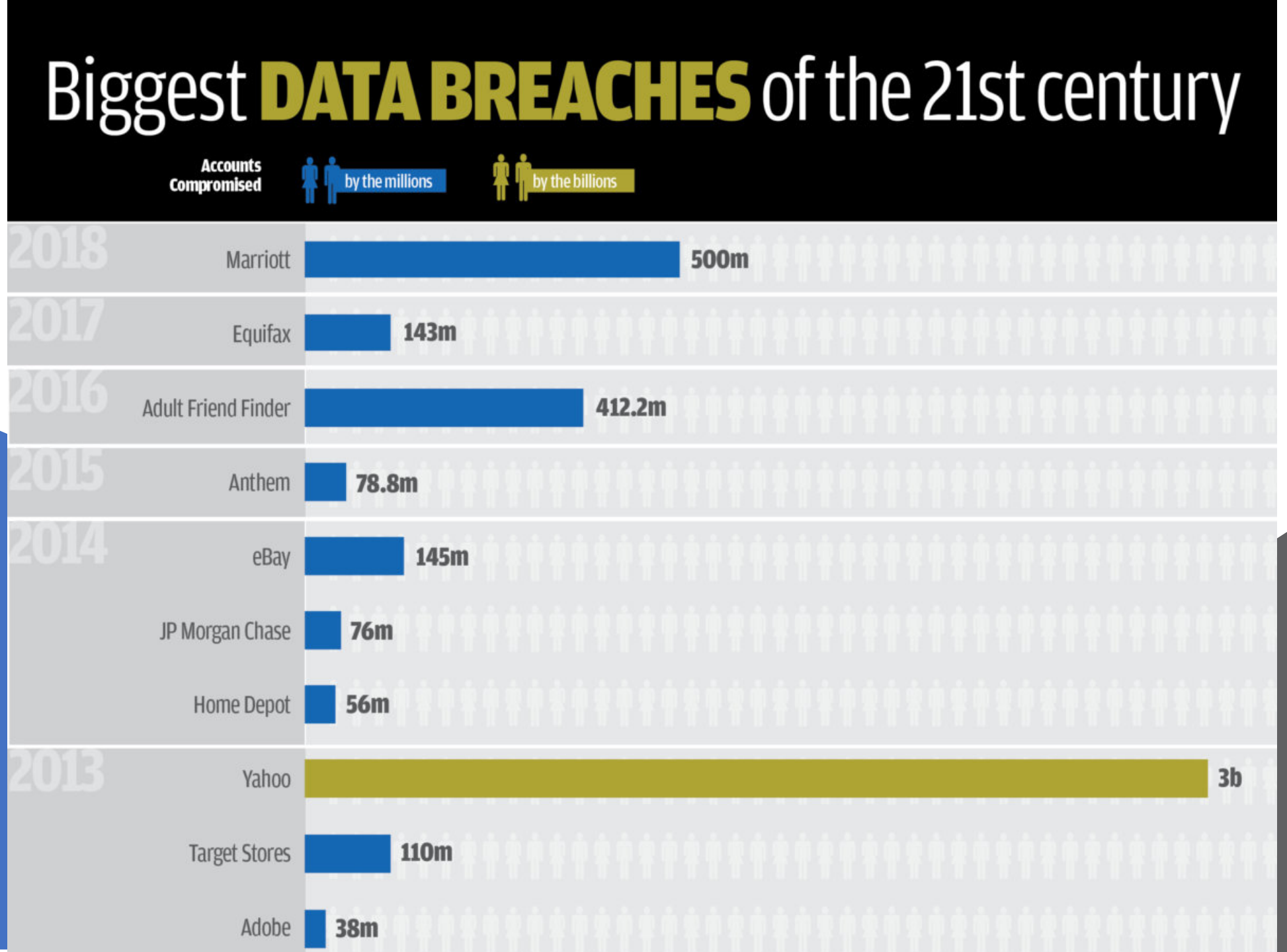
147 MILLION PEOPLE HACKED

Cybercriminals Use This Data To:

- Open credit cards and take out loans in your name.
- Steal your tax refund by filing a return with your name.
- Create highly targeted phishing scams to access your bank account, e-mail, computer and network.

COMPUTER DEPOT INC.
BUSINESS SOLUTIONS

Biggest DATA BREACHES of the 21st century



COMPASS

IT SECURITY

- Separate your Home network from you Work Network
- Use Strong WIFI Encryption
- Regularly Update firmware on your router
- Use enterprise level endpoint protection and VPN software

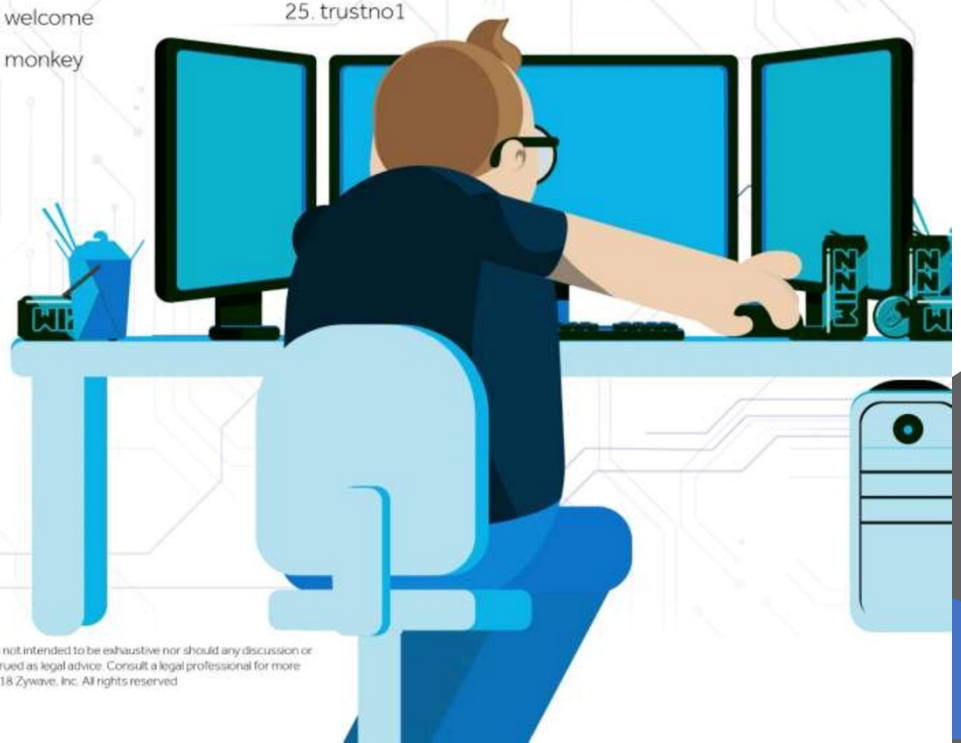
COMPUTER DEPOT INC.
BUSINESS SOLUTIONS

25 Most Commonly Stolen Passwords

THE CRAIN GROUP

Protect yourself—and your company—by making sure you're not using one of the top 25 most commonly stolen passwords of 2017, as determined by IT security firm SplashData.

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou
11. admin
12. welcome
13. monkey
14. login
15. abc123
16. starwars
17. 123123
18. dragon
19. passw0rd
20. master
21. hello
22. freedom
23. whatever
24. qazwsx
25. trustno1



COMPASS

A STRONG PASSWOR

- Use a minimum password length of
- Include lowercase and uppe symbols if permitted.
- Generate passwords
- Avoid using th e user accounts a /or software systems)
- Avoi ords r sequences, al information
- ith the user or the account.
- oid using that t intances might know to be associated wi e user.
- Do not use passwords which co mple combination of the aforementioned weak components.

NEVER MIND ALL THAT-
USE LASTPASS &
USE 2FA
NEVER REUSE PW

PHYSICAL SECURITY

- Use a Dedicated “Work” Room W/ Lockable Door
- Do NOT allow anyone else to use your Work Computer
- Be sure Laptops are encrypted and that your screen is set to automatically log out
- Print as few Docs as possible, shred ASAP