SOCIAL NETWORKING

OH THE PAIN OF IT ALL…

WHY SOCIAL MEDIA

- In 2017, the total paid by individuals to attackers as a result of malware and attacks is estimated at $5 Billion (2018, Merill Lynch).
- Business loss totals are estimated at $325 Billion (2018, Bank of America).
- These are only estimates.
- Some attacks and losses go unreported, and as such do not allow actual loss calculations.

HOW DO ATTACKS TAKE PLACE?

- Vulnerabilities of Social Media:
  - Poor passwords or lack of updated/changed passwords
  - Unprotected information exposure
  - Posting of pertinent information that should not be made public
  - Sharing of information – leads to phishing and spear phishing campaigns (2018, CSO online)
  - Hackers view social media as a target rich environment where people have a very low guard. It provides an opportunity to gather information that the attacker can use.

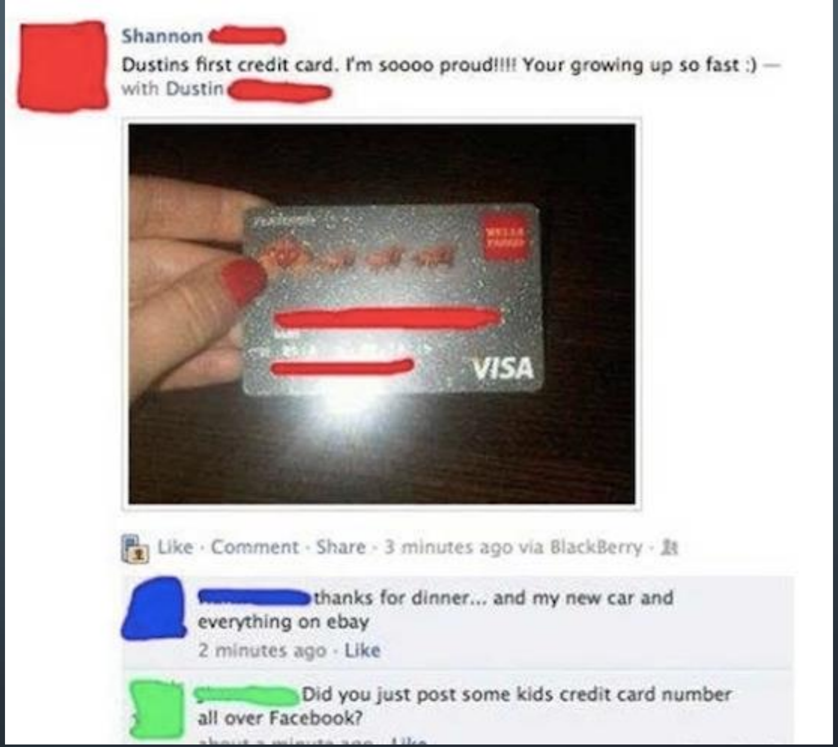
SOCIAL MEDIA RESOURCES FOR HACKING

- Social Media use has increased over the years.
- There is an assumption of interacting with others without risk.
- Social Media engages third party vendors and applications with privacy policies outside that of the provider.
- Personal information, tracking cookies, and other web resources can be tracked.
- Twitter top platform of choice for “Proof of Concept” hacking attacks and defenses.
- Malware apps and information is tweeted nine times more than just a public exploit and 18 times more than all other vulnerabilities (2018, CSO online)

WHAT ARE THE ATTACKS?

- Phishing or Spear Phishing: a means to target an individual or group of individuals with the intent to steal money or confidential information. Use anything of value against the target (person or business).
- Fake accounts to associate with in Social Media: Robin Sage account designed to actively push to request connections with hundreds of unsuspecting users. Once established, access to otherwise private information is possible.
- Celebrity name misuse: registering accounts under fictitious names to spread misinformation or rumors, or to attract new followers which later can be spammed.
- Site compromise: attacker takes or compromises the providers site which presents itself as a valid site capturing login information to use later against the account owner.
- Spread of Spam or Malware.

SOCIAL MEDIA BAD IDEA EXAMPLES



[redacted] Shannon [redacted]

Dustins first credit card. I'm soooo proud!!!! Your growing up so fast :) — with Dustin [redacted]

[redacted]

[redacted]

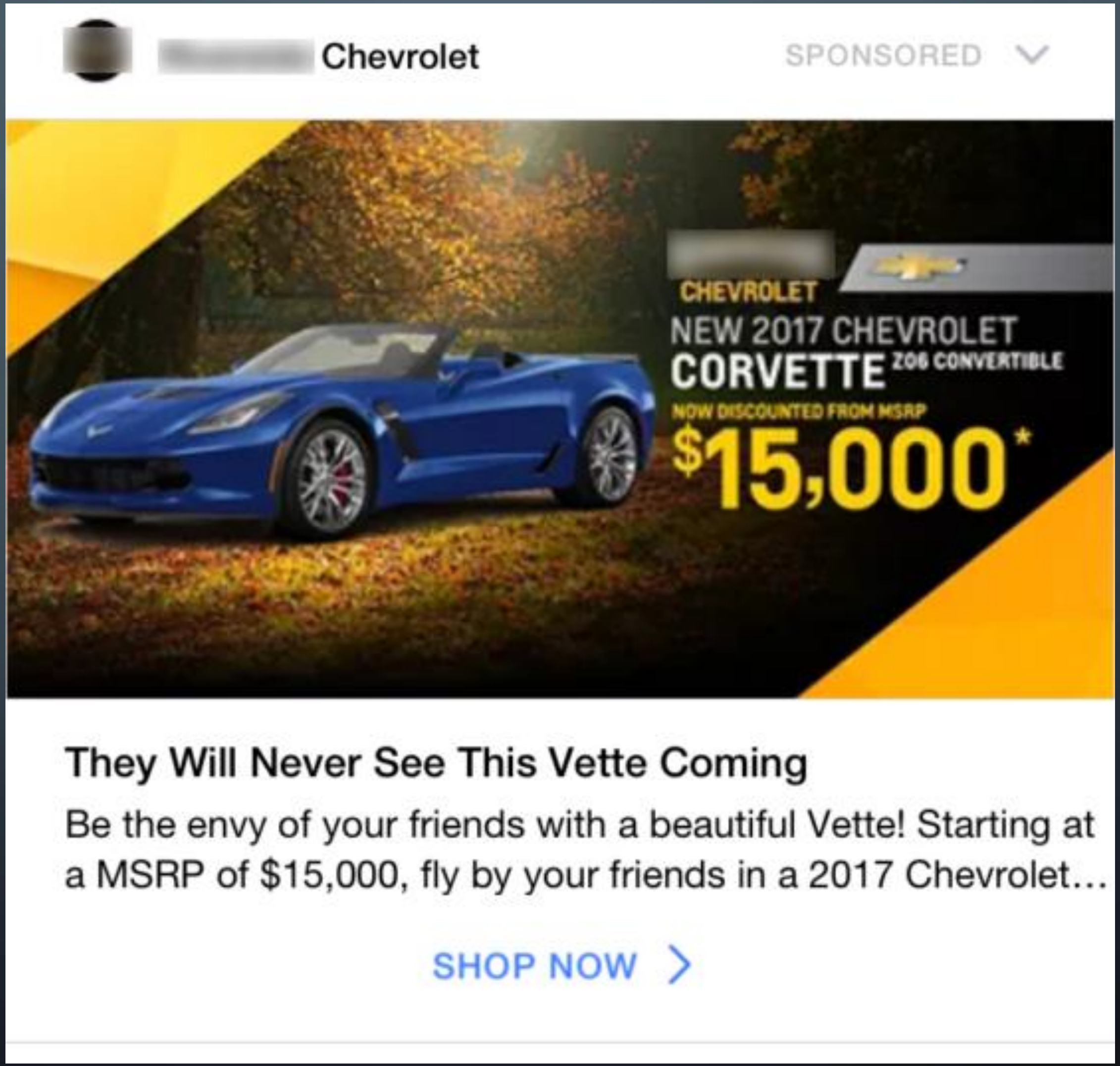
Like · Comment · Share · 3 minutes ago via BlackBerry ·

[redacted] [redacted] thanks for dinner... and my new car and everything on ebay

2 minutes ago · Like

[redacted] [redacted] Did you just post some kids credit card number all over Facebook?

SOCIAL MEDIA BAD IDEA EXAMPLES



[redacted] Chevrolet

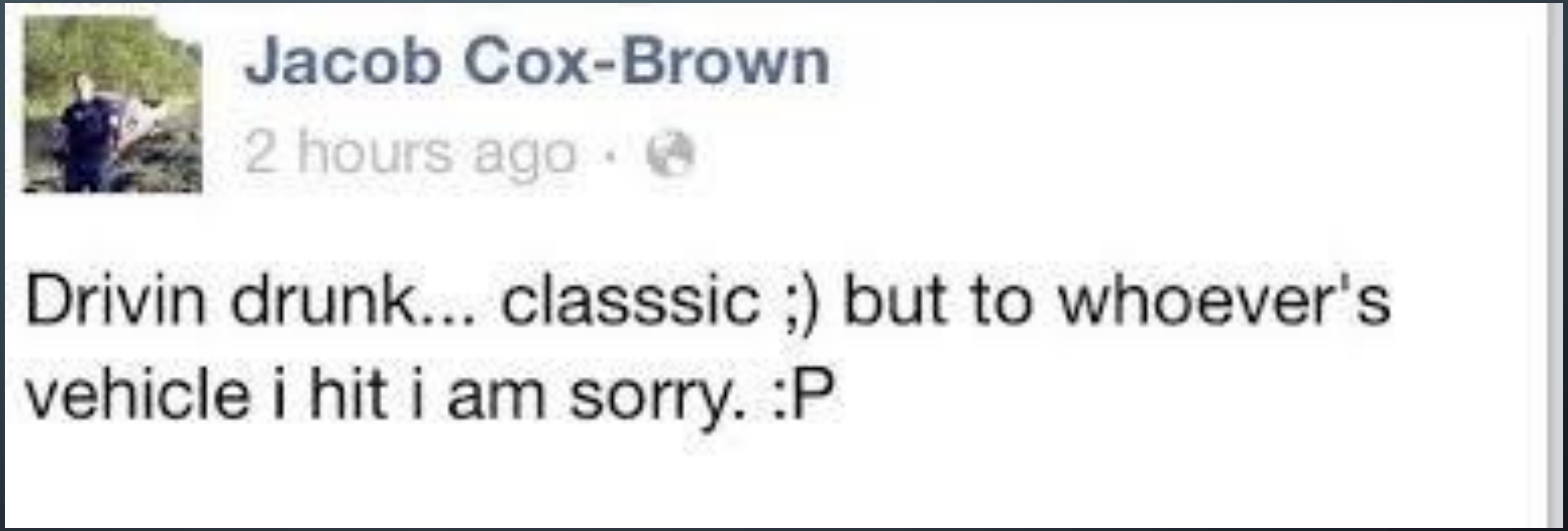
SPONSORED

They Will Never See This Vette Coming

Be the envy of your friends with a beautiful Vette! Starting at a MSRP of $15,000, fly by your friends in a 2017 Chevrolet…

SHOP NOW >

SOCIAL MEDIA BAD IDEA EXAMPLES

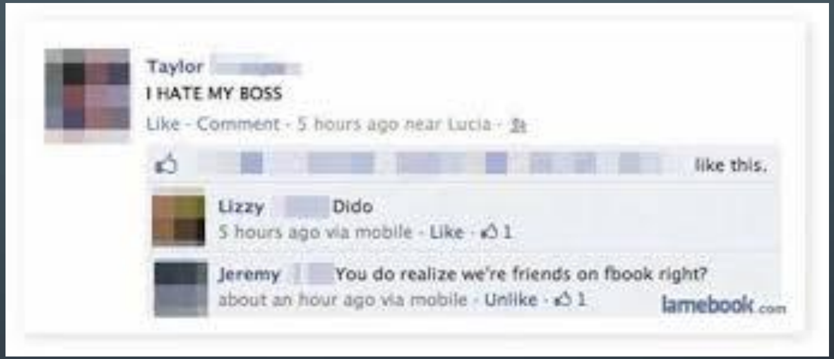


Jacob Cox-Brown

2 hours ago ·

Drivin drunk... classsic ;) but to whoever's vehicle i hit i am sorry. :P

WORST POSSIBLE MISTAKE



Taylor [redacted]
I HATE MY BOSS
Like · Comment · 5 hours ago near Lucia ·

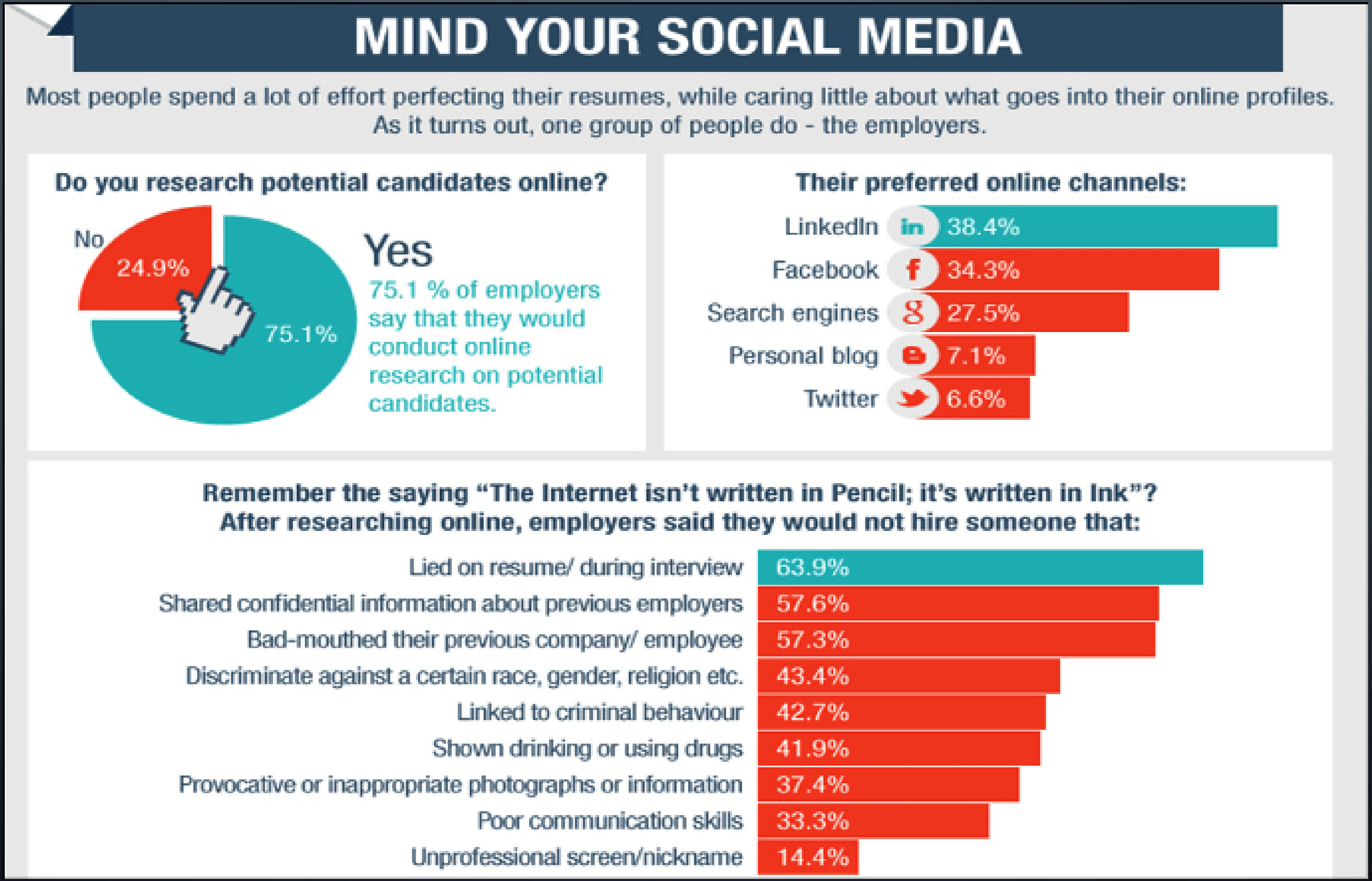
[redacted] like this.

Lizzy [redacted] Dido
5 hours ago via mobile · Like · 1

Jeremy [redacted] You do realize we're friends on fbook right?
about an hour ago via mobile · Unlike · 1

lamebook.com

SOMETHING TO CONSIDER



MIND YOUR SOCIAL MEDIA

Most people spend a lot of effort perfecting their resumes, while caring little about what goes into their online profiles. As it turns out, one group of people do - the employers.

Do you research potential candidates online?

Yes

75.1 % of employers say that they would conduct online research on potential candidates.

Their preferred online channels:

LinkedIn	38.4%
Facebook	34.3%
Search engines	27.5%
Personal blog	7.1%
Twitter	6.6%

Remember the saying "The Internet isn't written in Pencil; it's written in Ink"? After researching online, employers said they would not hire someone that:

Lied on resume/ during interview	63.9%
Shared confidential information about previous employers	57.6%
Bad-mouthed their previous company/ employee	57.3%
Discriminate against a certain race, gender, religion etc.	43.4%
Linked to criminal behaviour	42.7%
Shown drinking or using drugs	41.9%
Provocative or inappropriate photographs or information	37.4%
Poor communication skills	33.3%
Unprofessional screen/nickname	14.4%

WHAT IS APPROPRIATE?

- Who can see your posts? Check privacy settings.
- Controversial? Think twice before sharing your political or controversial views.
- Offensive? Triple check before you post anything that could be offensive to others.
- Negative? Avoid foul language, gossip, and negative remarks. (Liable versus Slander)
- Appropriate? A picture says a thousand words. Avoid drinking (including posts with solo cups), illegal behavior, and posts that are in bad taste.
- What should you post? Demonstrate personality and involvement; appropriate content is beneficial (to you the individual or a business). Show your clubs, organizations, sporting events, and other positive interests. Ask yourself, "Would I want my future employer to see this?“
- Posting announcements personal in nature (i.e. travel plans, getaways, vacations, and location information) is not encouraged. “Going on a cruise, see you all in a week!”

PRIVACY SETTINGS

- How much information is exposed to the public?
- Friends and contacts expand the list of potential attack candidates. How secure are they and what kind of exposure do they present for you?
- How easy is it to crack you weak password?
- When was the last time you changed your password and do you know how?
- Never share your password – no one needs to know it but you!

MALWARE

- Hacking a person is so much easier than hacking a business. It’s all about financial gain, it’s nothing personal.
- Poor practices and laziness: “Single Sign On” Password practices.
- Uneducated or unprepared for attacks. Web links or online requests, phishing, spam, or “online free gaming.”
- Links opened to Web sites or games – malicious code running or false site. User’s system becomes infected with malware: encryption of files, stolen cookies, data, or other artifacts.
- Verify any email, links, or information from someone you know and don’t know. It’s easier to ask if they sent it and be a little embarrassed than to be financially broke.

I'VE BEEN HACKED…!

- Change password(s) immediately. Do not wait and do not under estimate potential or threat from a stolen identity/password.
- Monitor any means of financial gain for any changes or small charges easily overlooked (GameStop is a common test). Call banks and financial institutions and report incidents of fraud, stolen identity, or to contest any unusual activity on accounts.
- Reach out to the Federal Government, local law enforcement agencies, and other online resources to assist in recovery.
- Always back up your data to a separate system that is NOT continuously connected to the computer.

WHAT'S IN A PASSWORD

- People are basically lazy – one password for all and all for one!
- Hackers count on this concept. One hack of a wireless router at home provides a plethora of passwords to other sites and resources.
- Passwords at home make their way into the work place and vice versa. This opens a another whole set of problems.

WHAT IS A GOOD PASSWORD

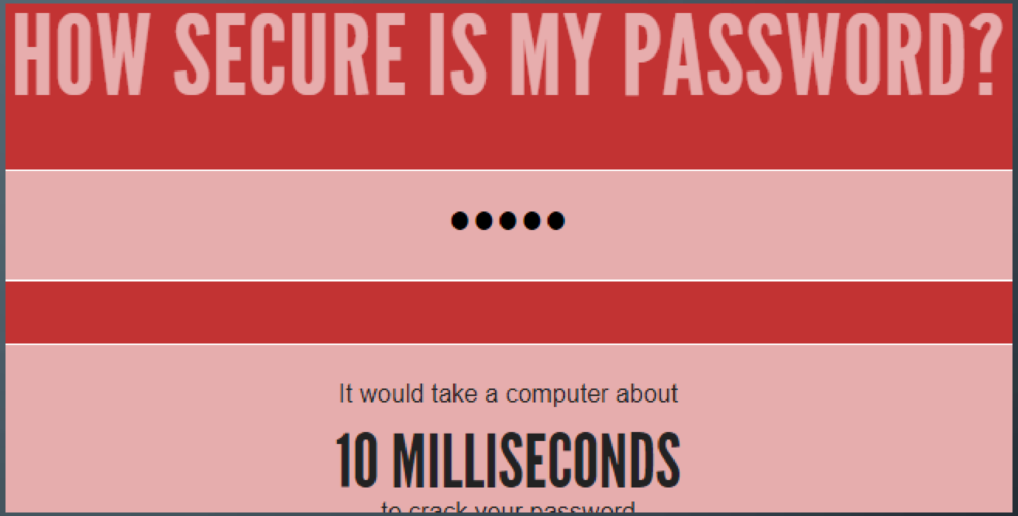
- At a minimum, 24 characters:
  - Upper case and lower case letters
  - Numbers
  - Special characters such as @ $ # ^ > < ? /
- Changed on a regular basis:
  - 45 days for any insurance, financial, medical, and banking
  - Do not recycle passwords: ILoveMyDog this time then ILoveMyDog1 next time.
  - Use a password generator
  - Store passwords in a password vault (with an option for online access).
    - Password access is encrypted
    - Failed attempts forces a wipe of the data.

HOW TO CREATE A GOOD PASSWORD

- Avoid using any personal information about you, your family, friends, favorite places, drink, food, or likes
- Use a “Pass Phrase” to start, then change up letters between upper and lower case, swap out vowels for numbers and special characters.
- **I love my dog skippy** becomes !l0v3MyDAWG$k!ppy…!
- Remember that a password is any combination of characters until the [Enter] key is pressed. Spaces can also be part of a password, just remember how many you included.

PASSWORD CRACKING

- Password without specialization:



HOW SECURE IS MY PASSWORD?

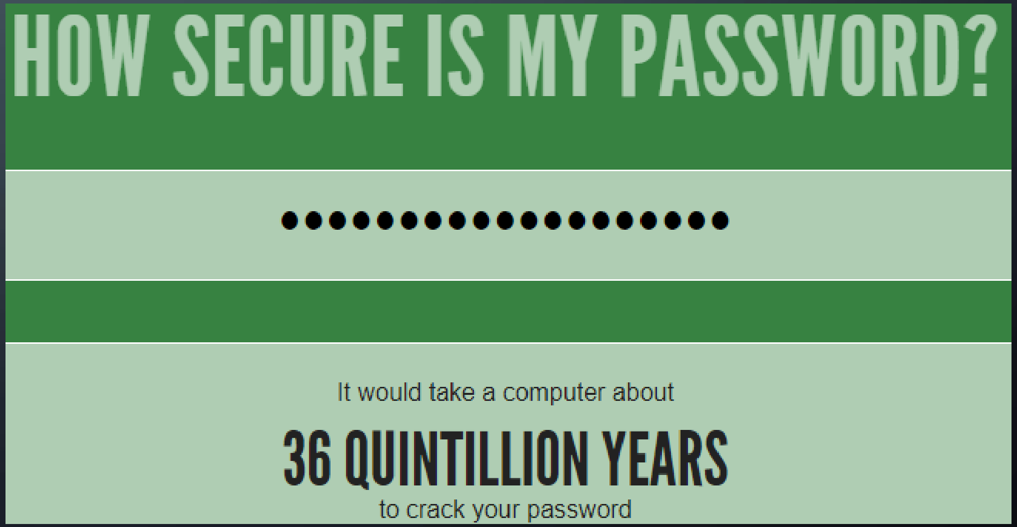
●●●●●

It would take a computer about

10 MILLISECONDS

to crack your password

- Password with specialization:



HOW SECURE IS MY PASSWORD?

●●●●●●●●●●●●●●●●●●●

It would take a computer about

36 QUINTILLION YEARS

to crack your password

PROTECT YOUR DATA AND YOURSELF

- Review online policy on Social Media sites.
  - Change settings to prevent unwanted viewing.
- Use strong passwords.
  - Change passwords regularly.
  - Use a password vault.
- Backup and store data separately.
  - Purchase an external USB 2.0/3.0 drive and back up records regularly.

QUESTIONS