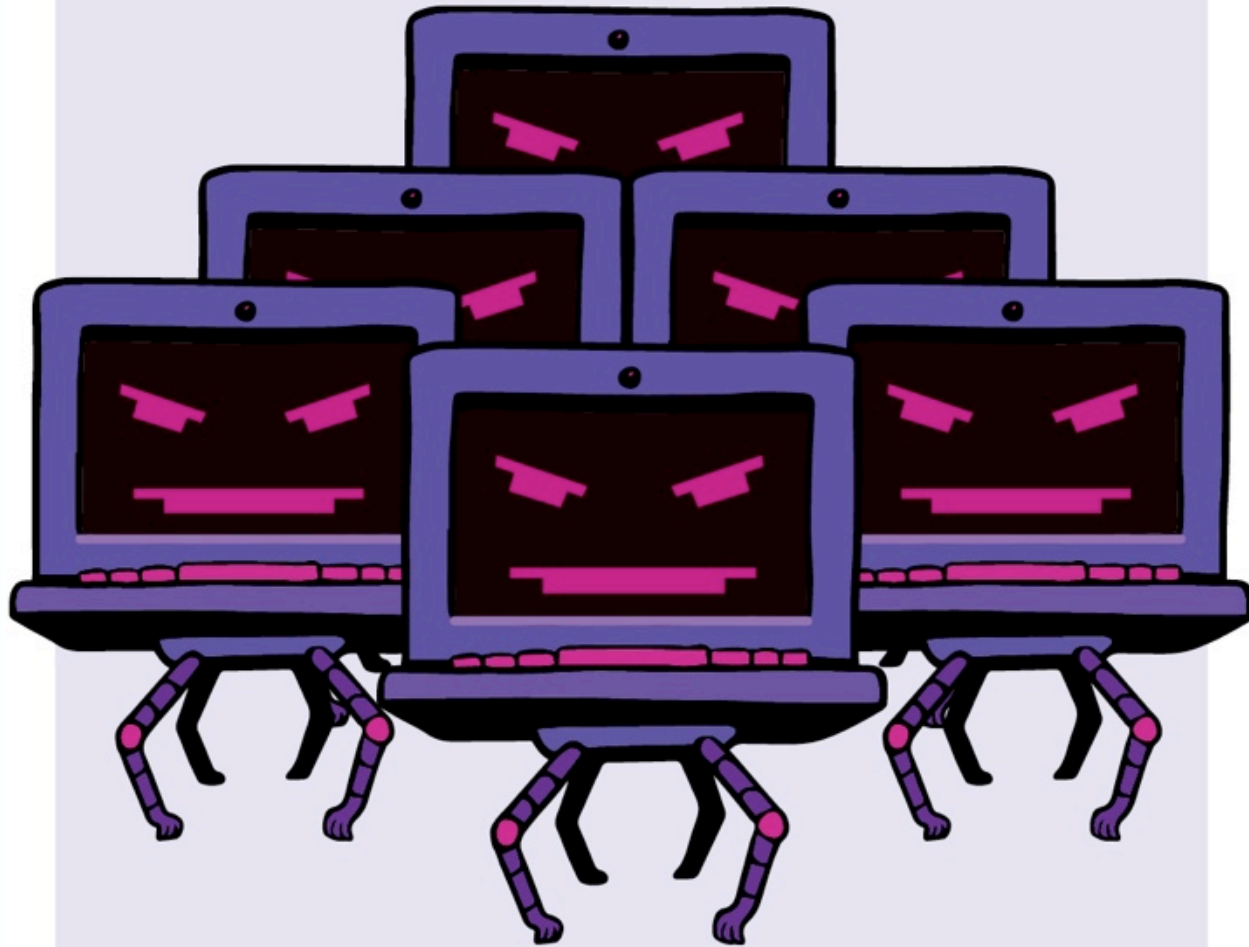


Know Your Trolls

KNOW YOUR TROLL

01



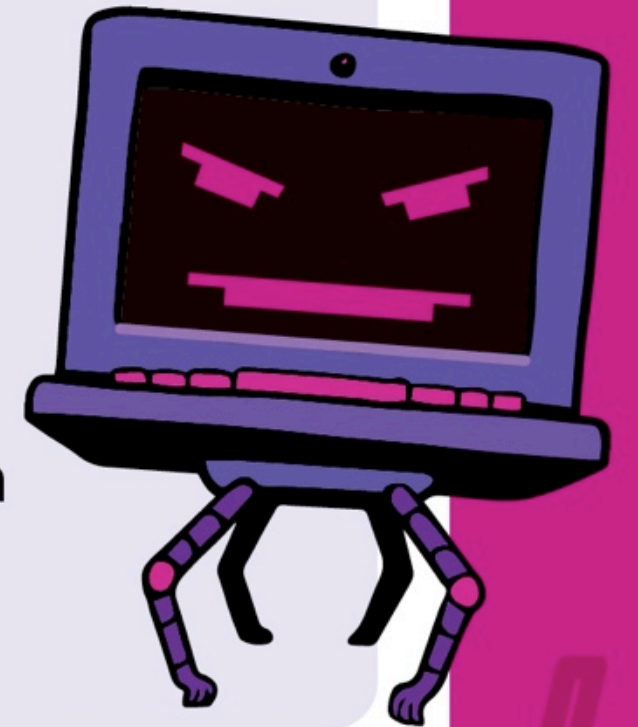
BOT NET

BOT NET

A Bot Net is a collection of devices, like computers or phones, that have been infected by hackers to work as a group. Botnets are used to send spam emails, overload websites, and send out fake information or propaganda.

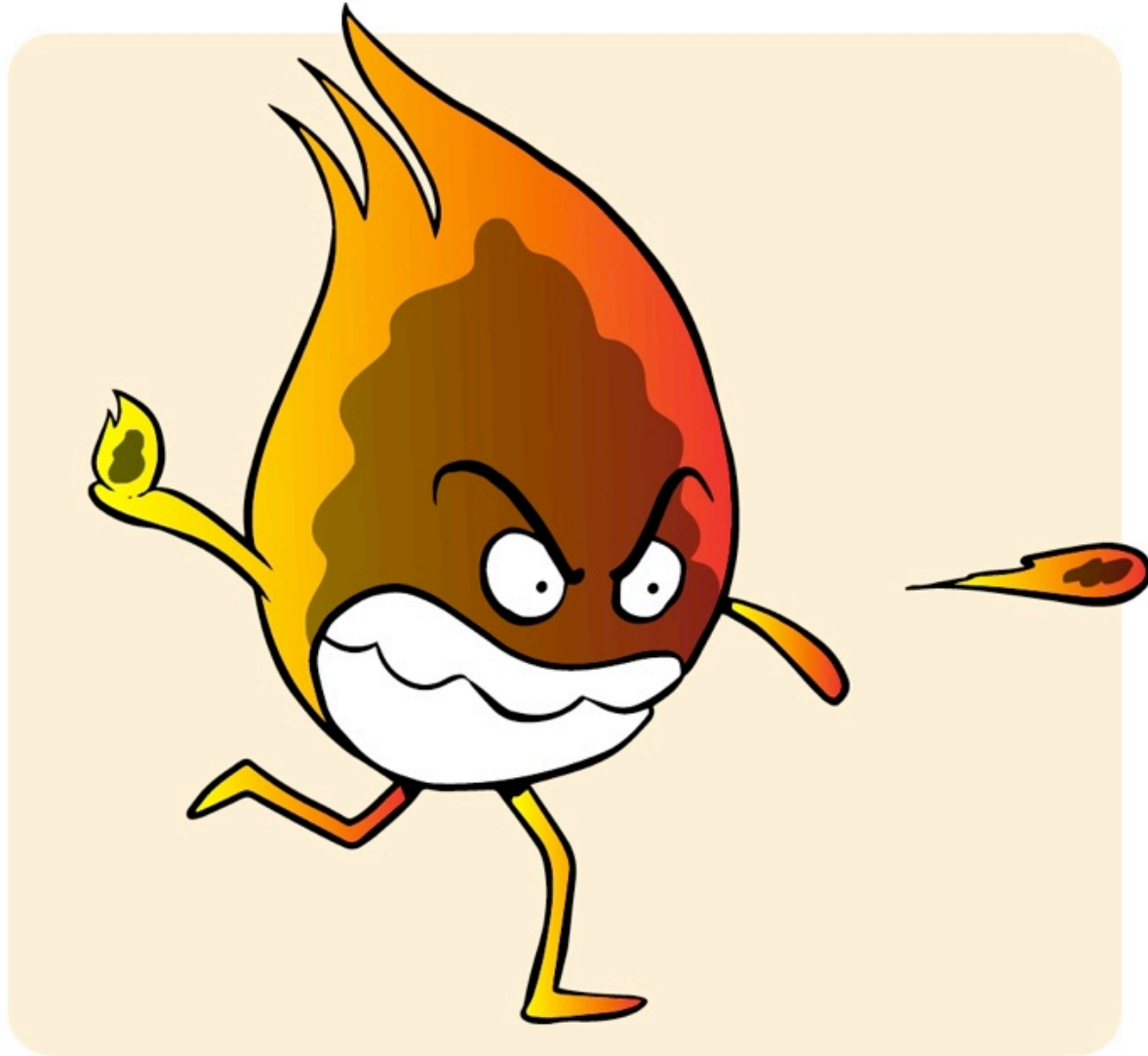
WEAKNESS

Protect your passwords, be careful what you click, and look out for bots pretending to be people. You can usually spot them from their fake bios and repetitive messaging.



KNOW YOUR TROLL

02



FLAME THROWER

FLAME THROWER

This guy wants war – A flame war. Flame wars result when multiple users engage in provocative responses to an original post, which is sometimes (but not always) flamebait. Flame wars often draw in many users – including those trying to defuse the flame war!

WEAKNESS

The best way to fight a fire is by cutting off its oxygen. Mute, Block, or just Log Out and walk away.



KNOW YOUR TROLL

03



MEDIA MAGICIAN

MEDIA MAGICIAN

This master illusionist can make fake news appear before your very eyes! Photoshopped images, manipulated media, and imposter content are the tricks up their sleeve.

WEAKNESS

Skepticism and critical thinking! Just because something looks legit, doesn't mean it is. Those photos could be fake, or stolen from a different article.



KNOW YOUR TROLL

04



THE SH*T POSTER

THE SH*TPOSTER

The Sh*tposter loves to post...well, sh*t. Their tone is aggressive, their content is ironic, and their memes are intentionally poor quality. All of it is designed to derail discussions and hijack dialogue, using minimal effort to get big emotional reactions. They're just here to stink things up.

WEAKNESS

It may look amateurish, but sh*tposting is an effective disinformation tool that's often used by troll farms. Block, report, and do not engage.



**By Failing to Prepare,
You Are Preparing to Fail**

Have Reinforcements Ready



Have Reinforcements Ready

You have many friends and allies because of who you are and what you do.

On your own channels, “Friend” or “Follow” profiles that have shown positive behavior and can also be allies.

Something to remember: your attackers will come from all over so your friends should too.

Assess Your Online Presence

Don't feed the trolls.

To prevent more negative comments, ignore negative, harassing, or bullying commenters:

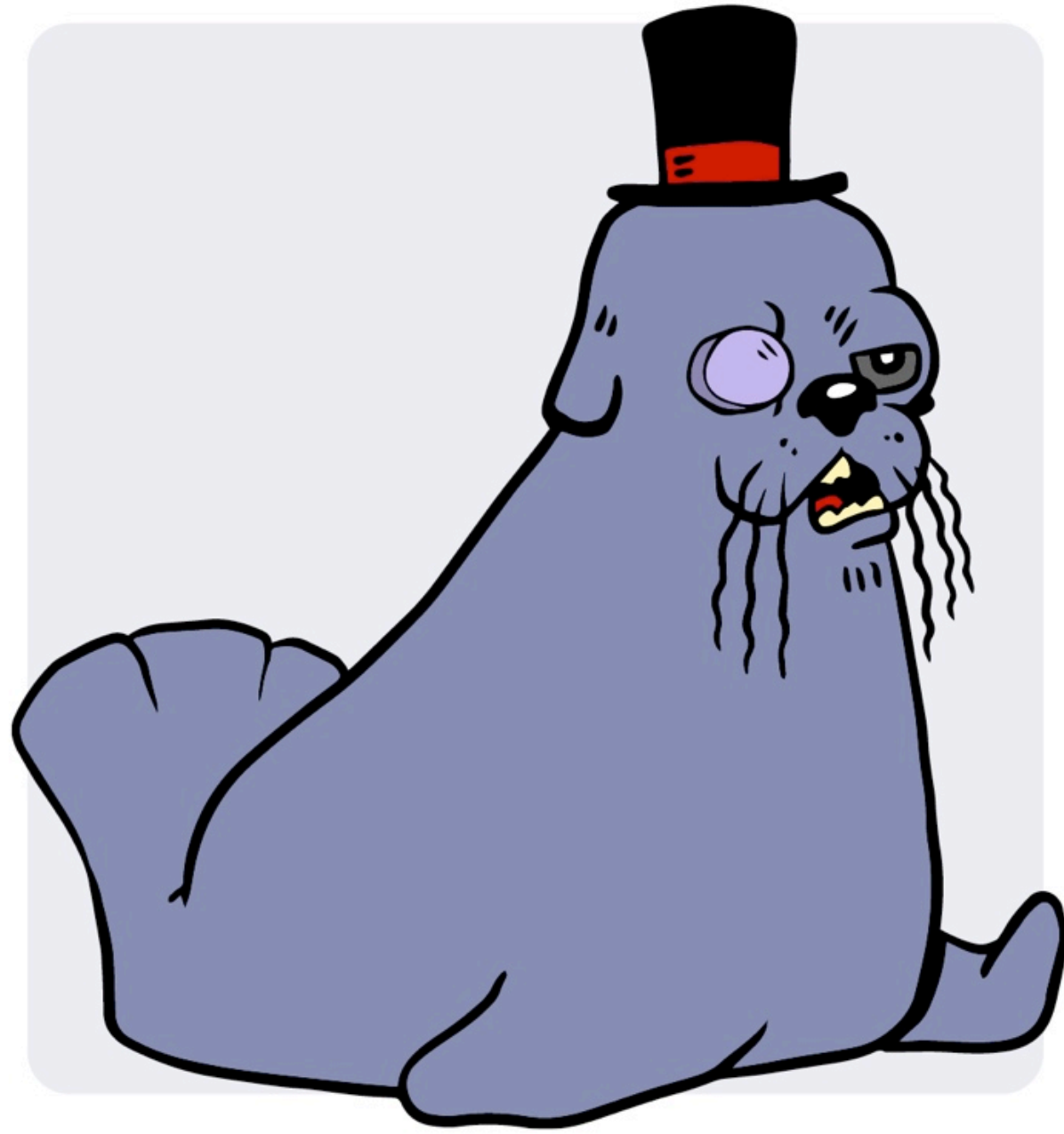
Avoid unnecessary fights and engage with caution: If you're going to engage with a comment, choose your conversations wisely based on the context.

Here are some things to consider:

- Is the person commenting in good faith? Are they open to a productive conversation? Are they egging you on?
- Do you know this person or trust them?
- Do they have a long history of anti posts and are they part of anti groups?

KNOW YOUR TROLL

05



SEA LYIN'

SEA LYIN'

"Sea Lioning" is a type of online harassment disguised as discourse. The Sea Lyin' may act civil and sincere, but their persistent questions and requests for evidence are really just bad faith attempts to troll.

WEAKNESS

The internet can be a great place for debate, when it's based on mutual respect and understanding. This guy just wants to argue. Mute or Block as needed, and let them Google that "evidence" for themselves.



KNOW YOUR TROLL

06



THE JOKESTER

THE JOKESTER

The Joker could be an online comedian or satirical news site, and usually they mean well – But if it has dishonest intent or gets shared out of context, the consequences are nothing to laugh about.

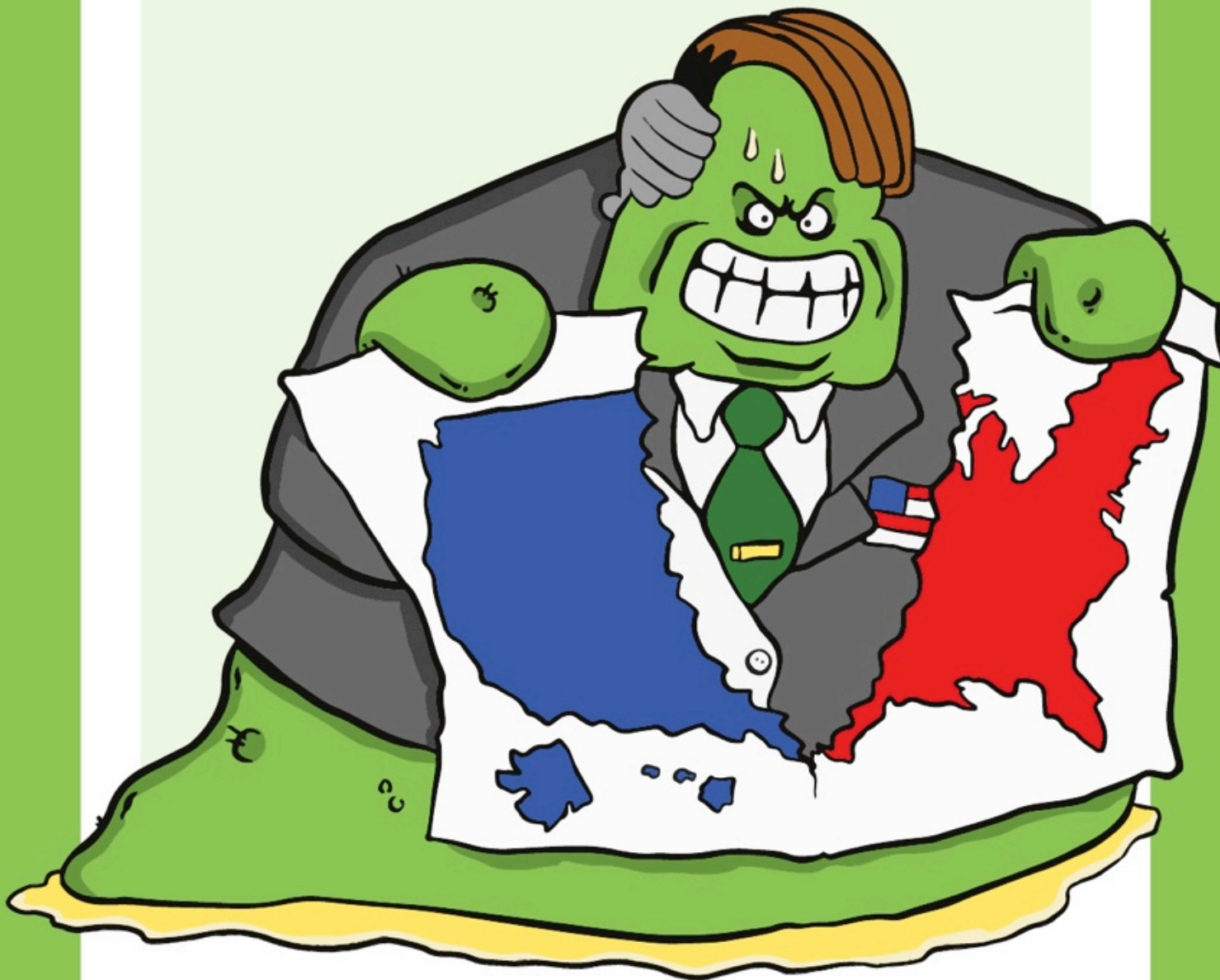
WEAKNESS

The Joker can be rendered harmless if you know how to take a joke, and more importantly how to spot one. Double check the source and verify the article before you turn yourself into a punchline.



KNOW YOUR TROLL

07



POLITISLICER

POLITISLICER

The Politislicer may be a troll, a political thought leader, or even an elected official, but their purpose is all the same – To sow division and spread misinformation by stoking our pre-existing political tensions.

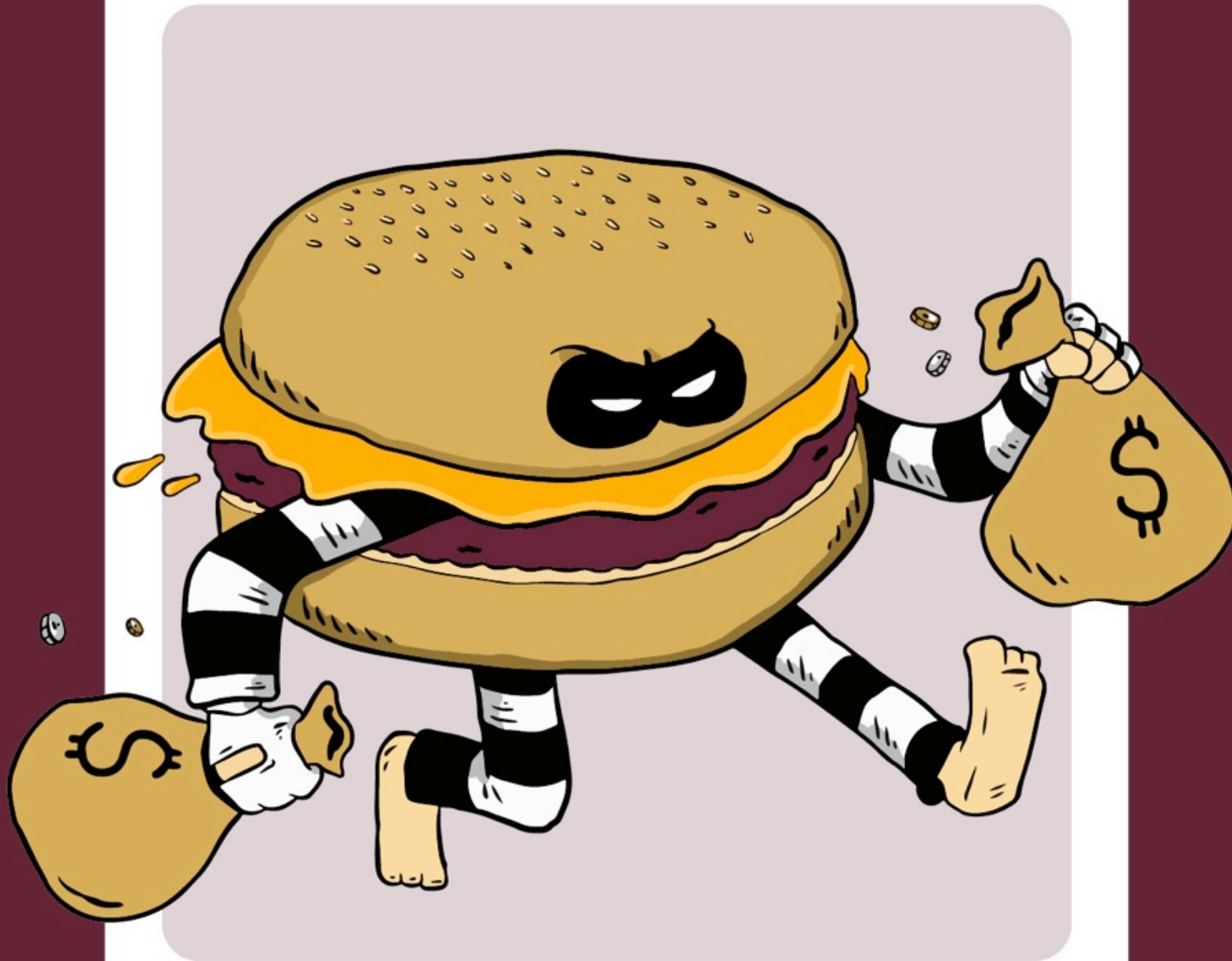
WEAKNESS

The Politislicer's tactics are a lot less effective when you're aware of your own biases, and fact-check news stories before you share them.



KNOW YOUR TROLL

08



SCAMBURGLAR

SCAMBURGLAR

When times get tough, scammers get scamming – And the bigger the crisis, the more misinformation they'll spread to make a quick buck. They'll invent fake charities to prey on your empathy, or pretend to be the IRS to prey on your fear, using phishing and imposter content as their tools.

WEAKNESS

Research a charity before you give, be careful what you click, and never give out personal information to strangers.

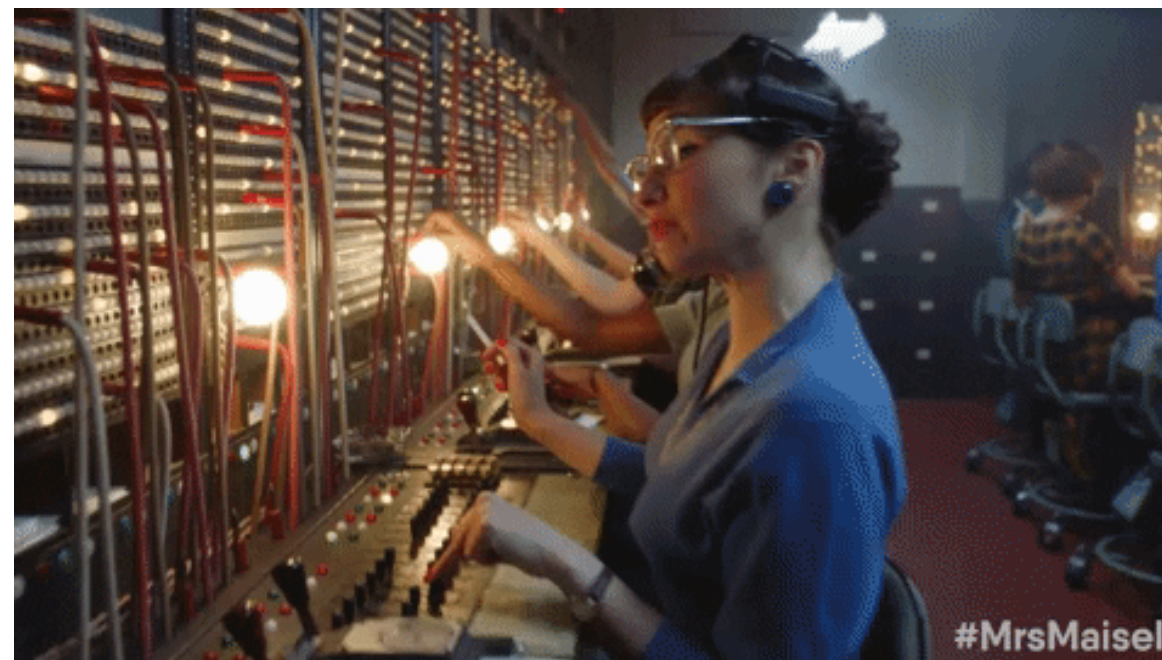


Prepare Your Team

Phones: train staff to recognize signs of an attack, how to respond, and when to notify leadership.

If your phones are ringing off the hook with negative, rude, or prank calls:

- If possible, ignore/silence the phone or turn it off
- If it's a line you must answer, determine if it's a negative call, and if so, hang up or politely dismiss
- Document the number of fraudulent phone calls and include phone numbers and messages



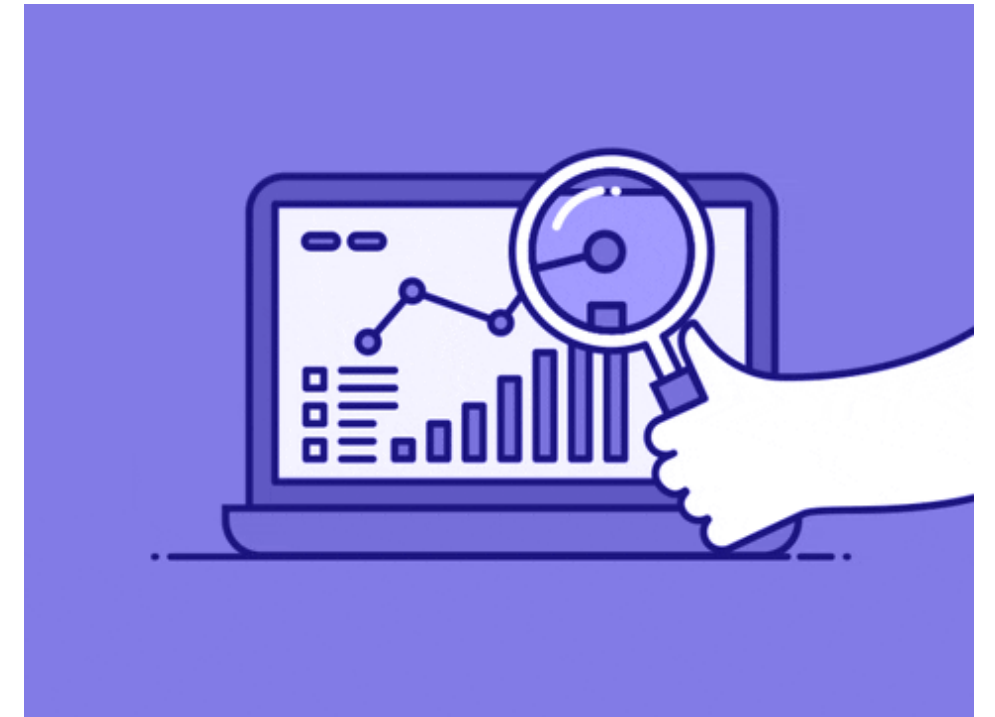
Recognize the Signs of a Digital Tsunami

Prepare Your Team

Know the signs of an impending social media attack.

Staff responsible for monitoring accounts should be trained to look for:

- A spike in or higher than usual volume of negative comments
- Unusually rude or mean comments from new accounts
- Links or screenshots of your page being posted in anti groups or by anti pages
- People in your pages' comments directing others to attack you
- Negative comments from suspicious, anonymous, or bot-like accounts
- Attackers contacting you through other platforms



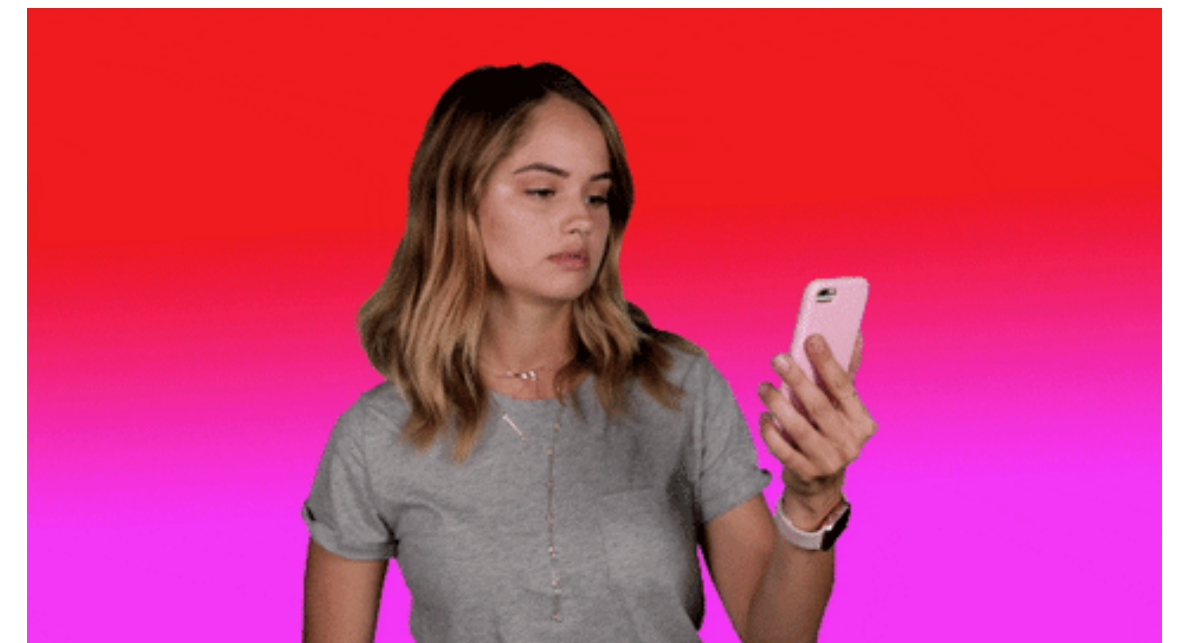
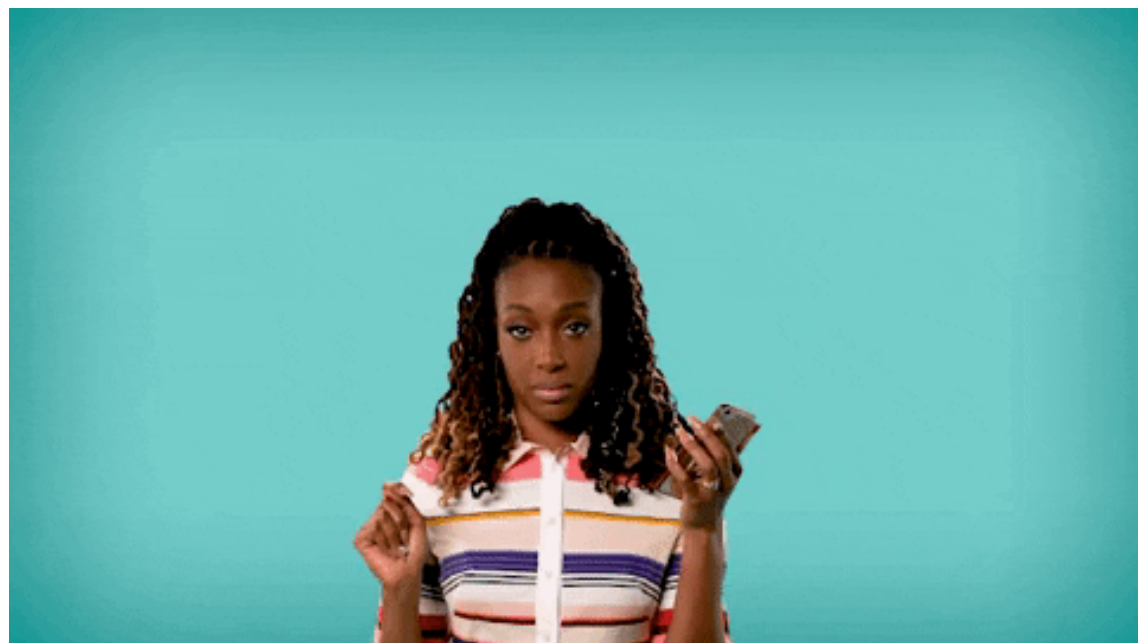
Prepare Your Team

Monitor online account security.

Turn on two-factor authentication for all accounts that support it.
Use strong, different passwords or a password manager.

Know your platform's settings in case of attack:

Know how to quickly limit or turn off comments, block offending accounts, make your profile private, report offending accounts, and delete offending comments.



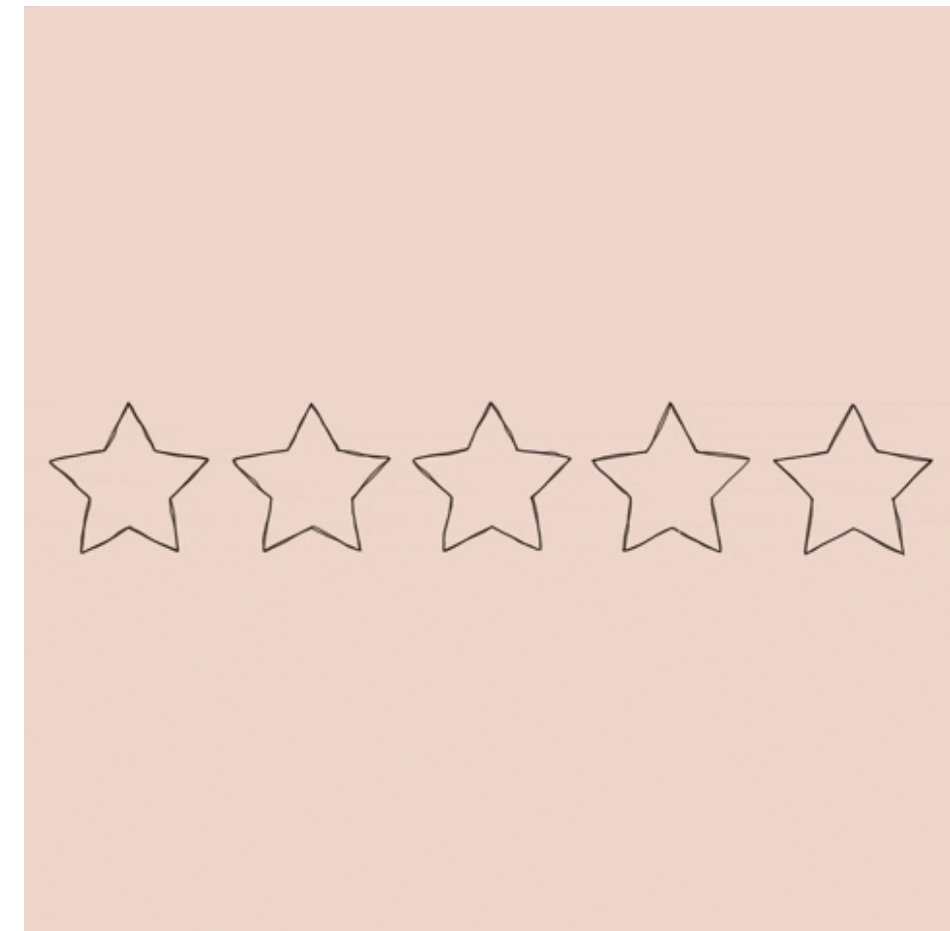
Prepare Your Team

Consider making your accounts private.

Claim your business online (Yelp, Google).

Enable email notifications—this way you'll know quickly if an attack were to happen

- Facebook
- Yelp
- Google My Business



Prepare Your Team

“Google” and “De-doxx” yourself

Doxxing is to publicly identify or publish private information about (someone) especially as a form of punishment or revenge. It is important to know if any of your personal information is publicly available online. This information can make you more vulnerable to being doxxed.

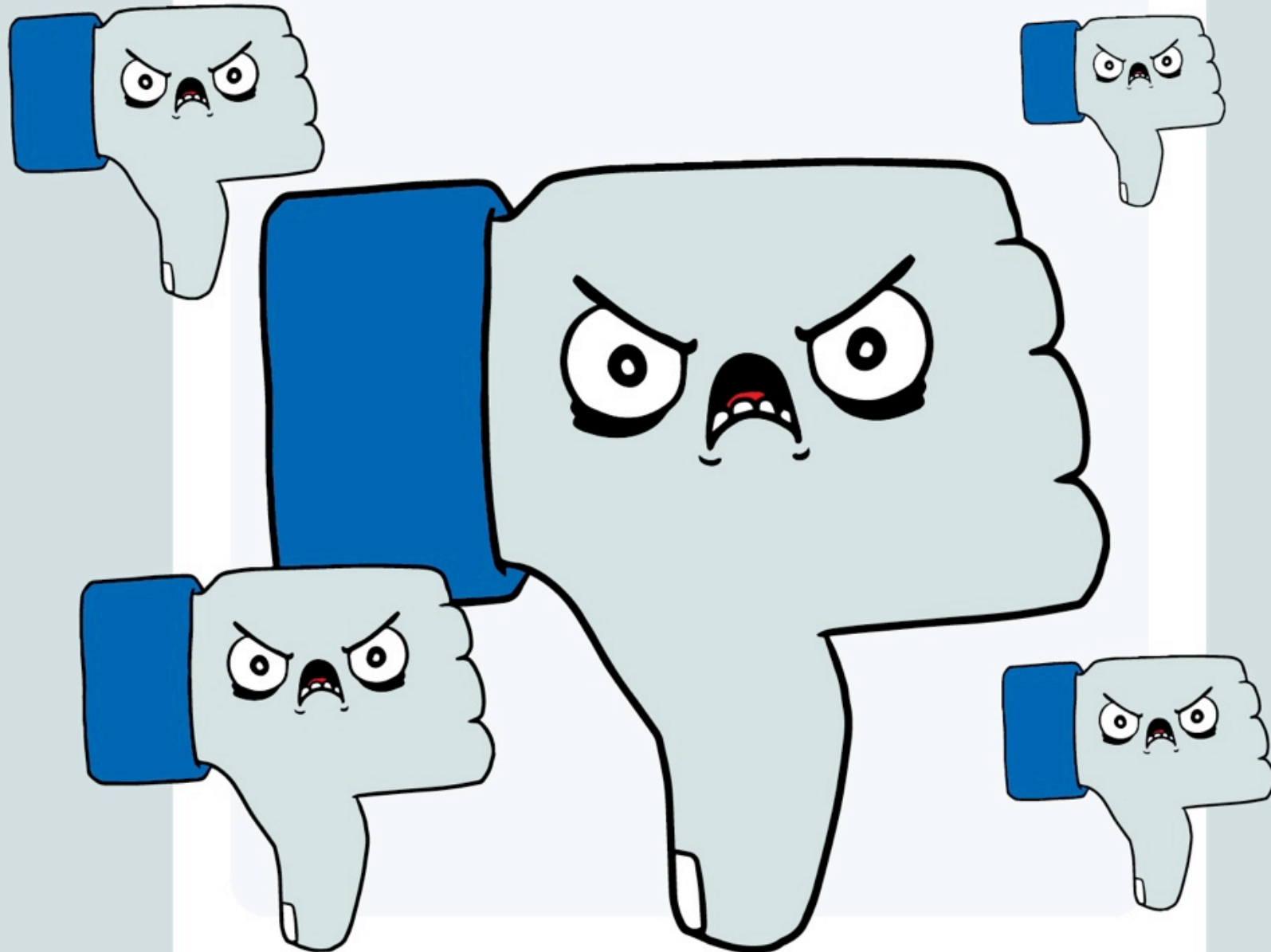
Search for yourself on search engines like Google and delete as much information as possible from the sources that come up

Remove your information from people-search or data broker sites

Make your social media private

KNOW YOUR TROLL

09



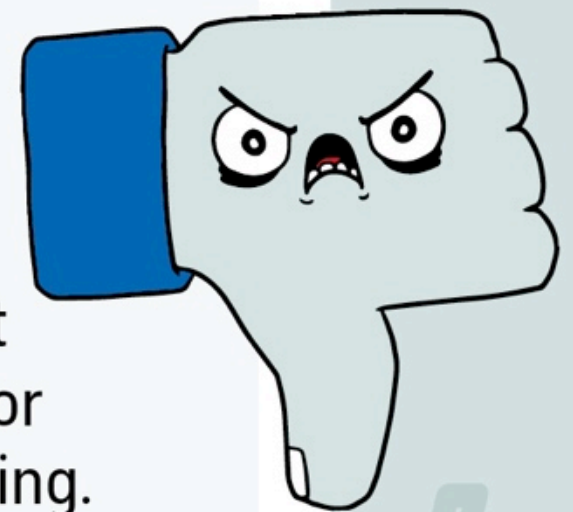
HATER-RATERS

HATER-RATERS

User generated review sites such as Yelp, Google Books and Trip Advisor have been used to publicly shame or punish businesses. Internet users are urged to “Review Bomb” with a barrage of negative reviews in order to punish corporate interests or businesses they dislike – Often with a political or cultural agenda in mind.

WEAKNESS

As misinformation tactics go, this one deserves 1-star. Just know that online ratings aren’t always deserved, and decide for yourself what’s worth supporting.



KNOW YOUR TROLL

10



ASTROTURFERS

ASTROTURFERS

Astroturfers may look like an organic, grassroots movement – But that grass is all fake. Through fake organizations and headline grabbing publicity stunts, astroturfing's real purpose is to mask the sponsors of their message, which tends to be a much larger entity that doesn't have the public's best interests in mind.

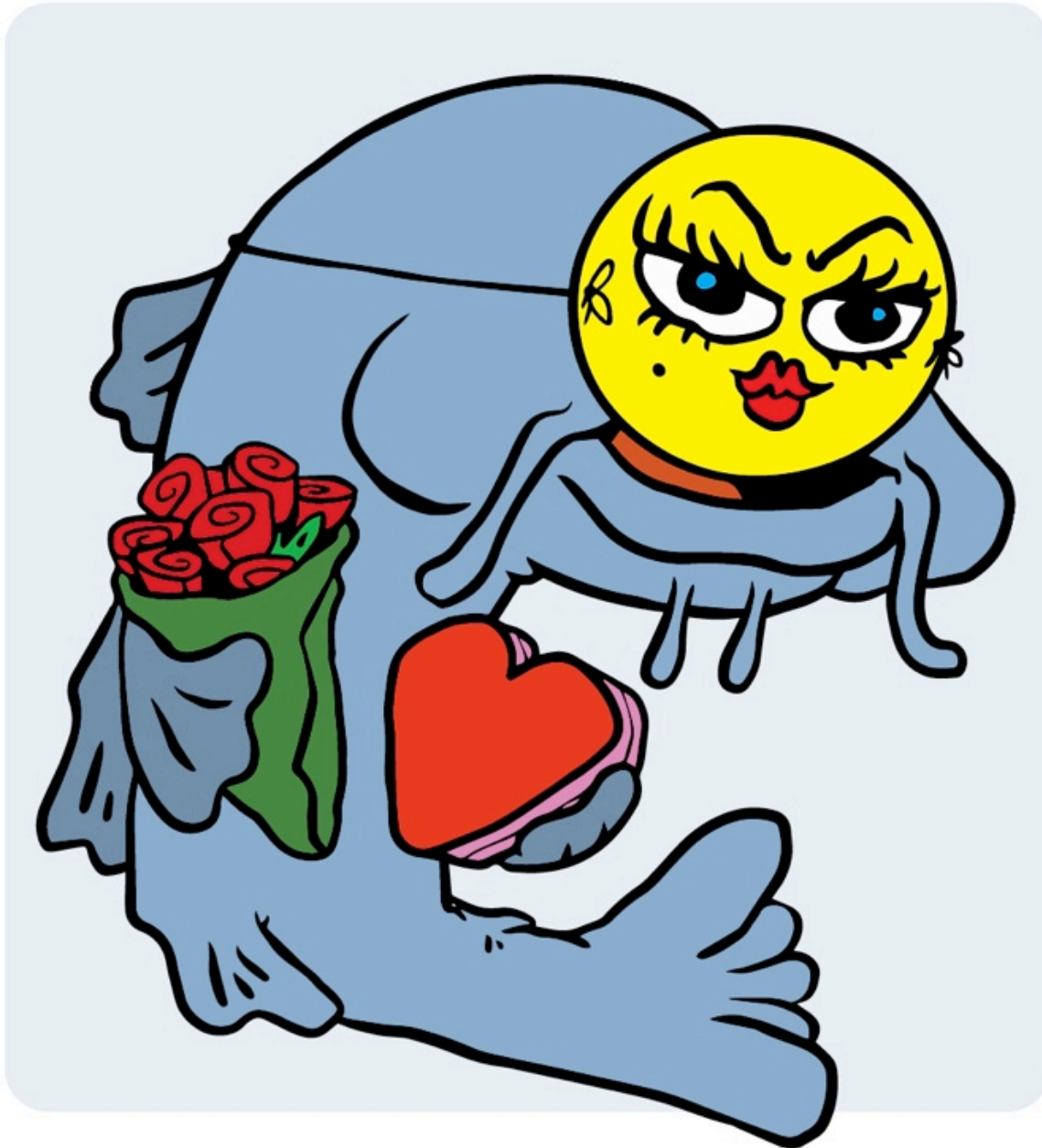
WEAKNESS

You can only spot astroturf by looking closely. If an organization isn't transparent about their financial connections, that's a big red flag.



KNOW YOUR TROLL

11



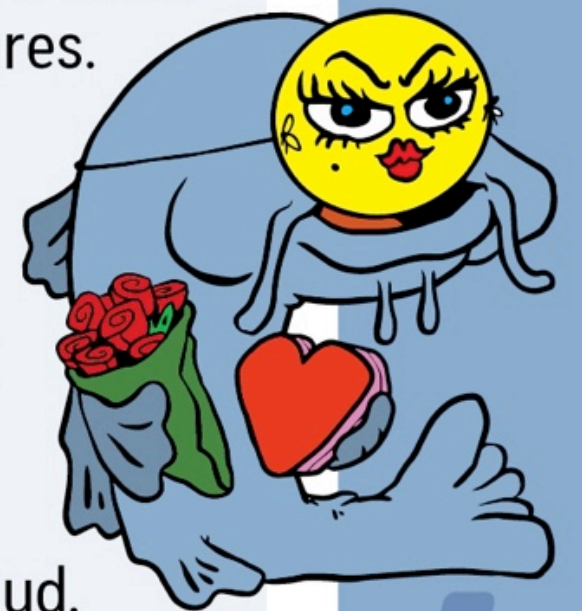
CATFISHER

CATFISHER

Catfishing is a deceptive activity where a person creates a fake identity on a social networking service, usually targeting a specific victim for abuse or fraud. Catfishing is often employed for romance scams on dating websites. Misinformation agents use similar tactics to lure users in with attractive profile pictures.

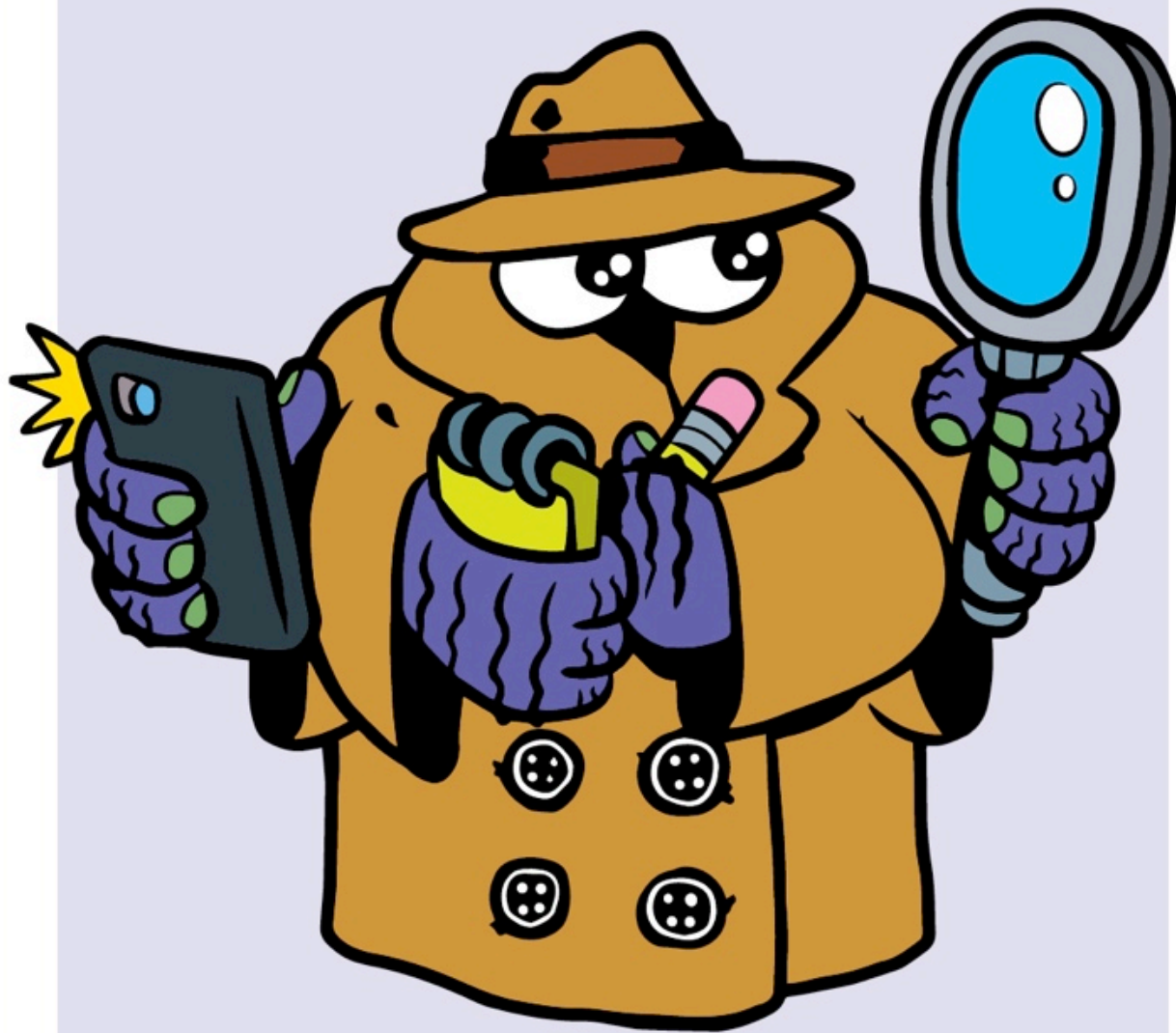
WEAKNESS

Don't be fooled by a pretty face. Be careful when entering an online relationship, and run a reverse-image search on those profile pics to expose fraud.



KNOW YOUR TROLL

12



DOXXER

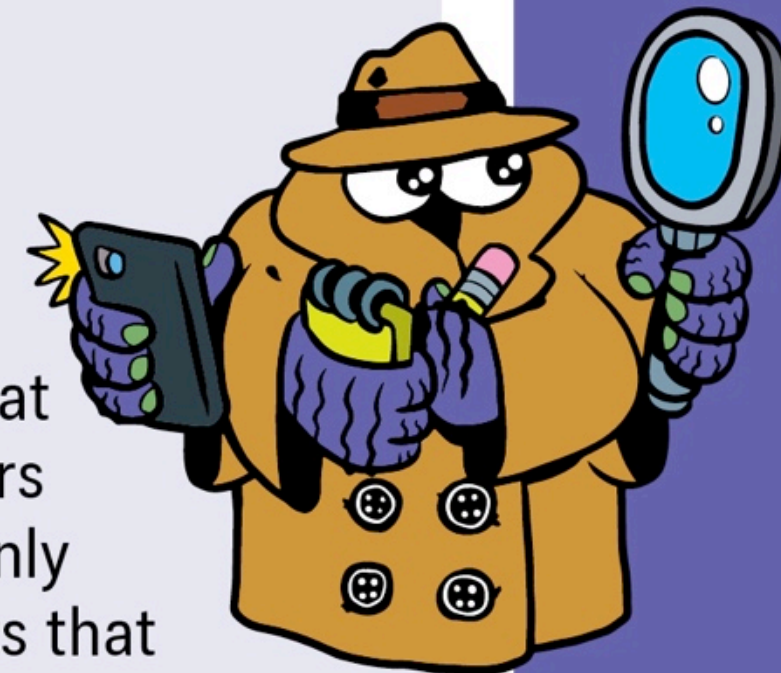


DOXXER

Doxing involves researching and posting personally identifiable information about an individual, like names, workplaces, and addresses, often with the intention of harming that person.

WEAKNESS

Be aware of how much personal info you share online, and how easy that info may be for strangers to access. Doxxer can only see the digital footprints that you leave out in the open.



Defend



1. Remember: You will overcome this and you are not alone.



6. Screenshot and save all attacks, including negative comments, fraudulent reviews, and other such content.



2. Ask for support.



7. Report and block attackers and delete negative comments.



3. Don't engage with attackers.



8. Claim your businesses on [Yelp](#) and [Google](#).



4. Turn off social media notifications.



9. Inform your employer/employees of the situation.



5. Increase your privacy settings on the platform and pages of the attack.



10. Take breaks to take care of yourself and your mental health.

KNOW YOUR TROLL

13



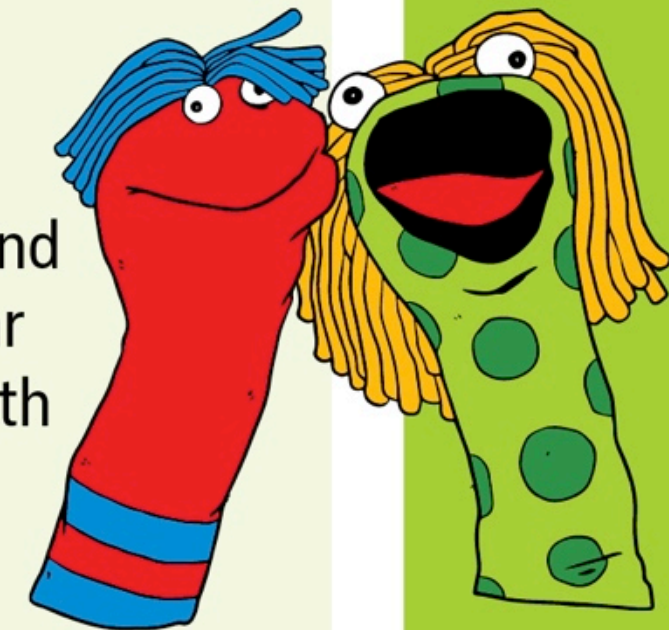
SOCK PUPPETS

SOCK PUPPETS

Sock Puppets are online identities used for purposes of deception. These identities can exist in large number, yet are controlled by a single person or group. This tactic creates the illusion of a false majority opinion that spreads and validates misinformation.

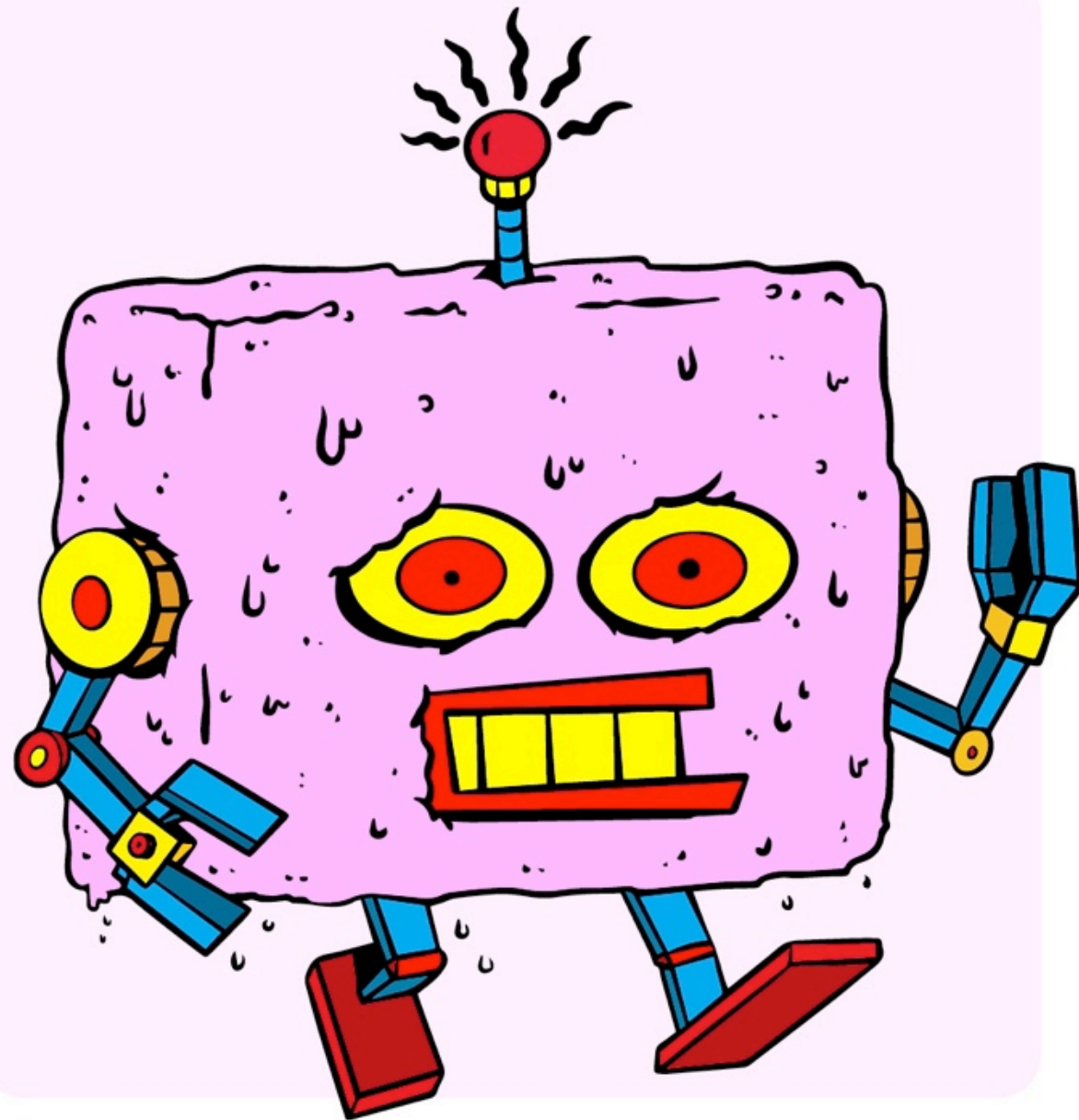
WEAKNESS

Sock Puppet content is low-quality, often abusive, and weirdly focused on a singular topic. You wouldn't argue with a sock puppet in real life, so don't do it online. Block, report, and keep scrolling.



KNOW YOUR TROLL

14



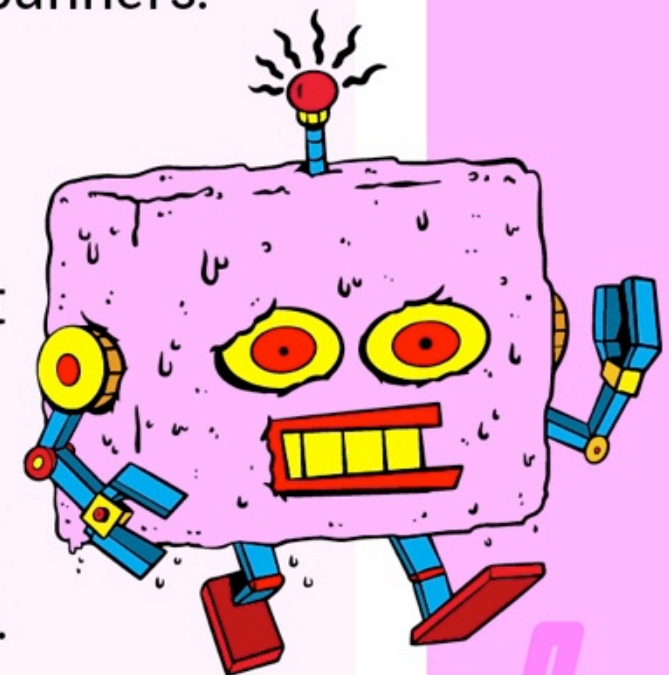
SPAMBOT

SPAMBOT

Spambots are programmed to primarily target community portals, blog comment sections, social media platforms, and data collection forms. They interfere with conversations, troll users, and insert unwanted advertisements, links and banners.

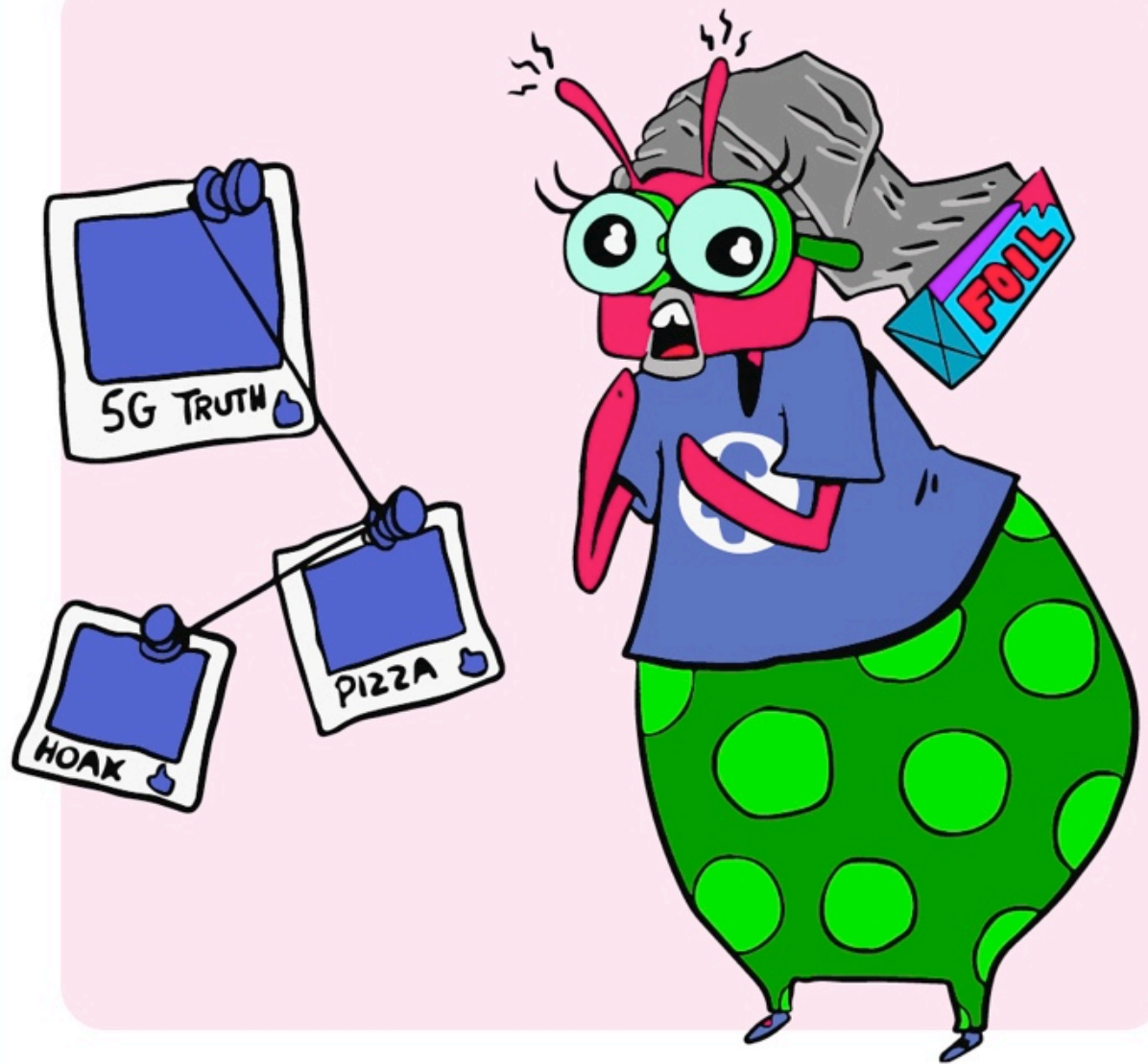
WEAKNESS

Block and report Spam when you see it, to prevent it from spreading. Better yet, adjust your security settings to prevent getting spammed in the first place.



KNOW YOUR TROLL

15



CONSPIRACY ANT

CONSPIRACY ANT

Not all misinformation spreaders are trolls and bots... Some of them are your friends and family! Chances are they started out with good intentions, but got caught up in the wrong Facebook Group, and soon began peddling conspiracy theories onto your timeline. It can happen to anyone if they aren't careful.

WEAKNESS

Don't take the bait, and don't be bullied. If you think you can reason with them, it's best to do so in a private, offline dialogue.



KNOW YOUR TROLL

16



JEER SQUAD

JEER SQUAD

When a brand, celebrity, or sometimes even a random person is deemed to have acted or spoken in a questionable manner, The Jeer Squad is right there on the frontline, riling up the crowd. They don't encompass all critics, just the ones who favor attention and punishment over understanding and justice.

WEAKNESS

Not all boycotts are bad, and online criticism can be deserved – But the performative nature of social media can push things to get mean-spirited and radicalized pretty quickly. Be aware of peoples' true intentions (as well as your own) and try not to get caught up in the dogpile.



Move Forward

Step by Step

Attacks can end gradually or rapidly, but either way you'll notice negative engagement decline when the attackers limit their engagement, are blocked, and lose interest. As you notice this, it is critical to take time to rest, clean up your pages, and get organized.

- Organize all screenshots and records from the attack
- Debrief with any staff, moderators, or family who have access to your page or witnessed the attack.
- Make sure to collect all evidence, assess access moving forward, and check on everyone's mental health – including your own.

KNOW YOUR TROLL

17



PSEUDO-SCIENTIST

PSEUDO-SCIENTIST

Who needs scientific evidence when you've got memes? Pseudoscientists use fake credentials to peddle their alternative facts, using tactics that range from irony and humor to straight-up falsified data. The only class they should be teaching is Scamology 101.

WEAKNESS

Critical thinking is a crucial part of the scientific process. Vet your information sources carefully, avoid miracle cures, and be wary of conspiracy theories.



KNOW YOUR TROLL

18



CLICKBAITER

CLICKBAITER

Made you look! Clickbaiter's content only has one purpose: To lure you in. His tacklebox includes false advertisements, sensational headlines, misleading thumbnail images, and all sorts of other nasty tricks to get your clicks.

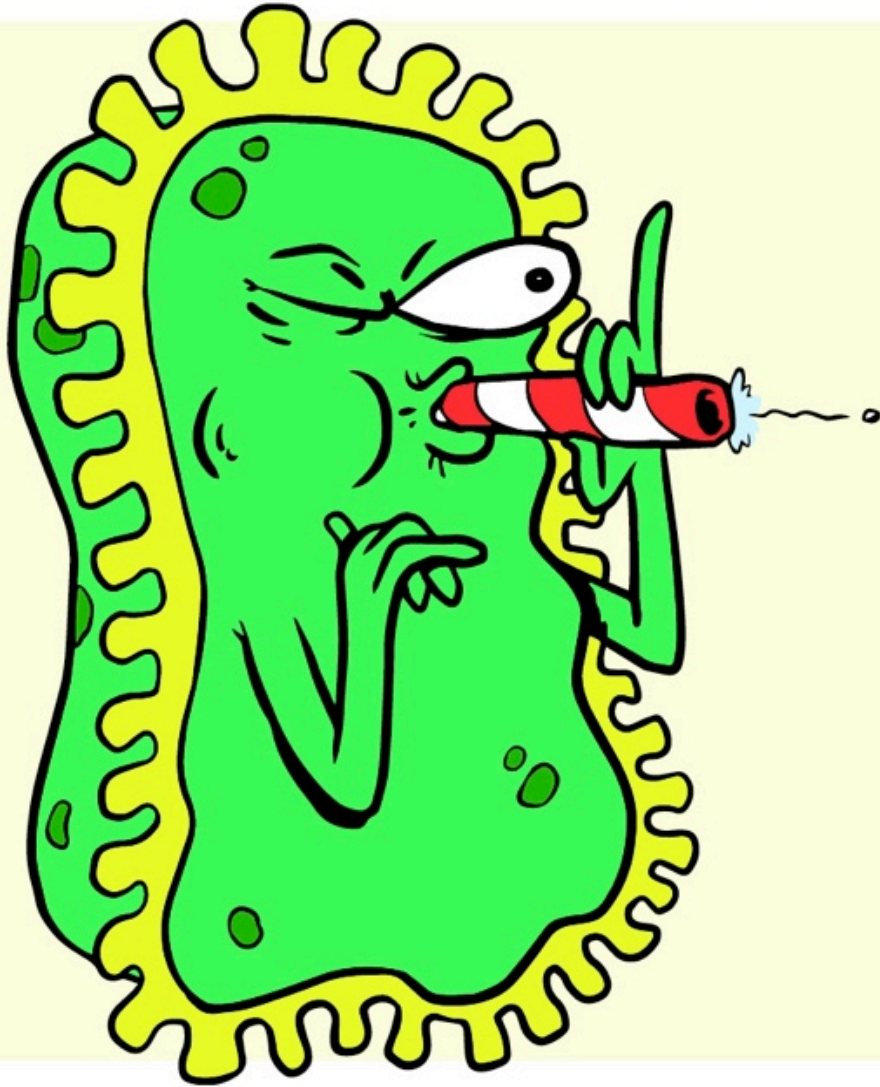
WEAKNESS

Attention is currency on the internet. Know what yours is worth and don't take the bait!



KNOW YOUR TROLL

19



MICRO-TARGETETER

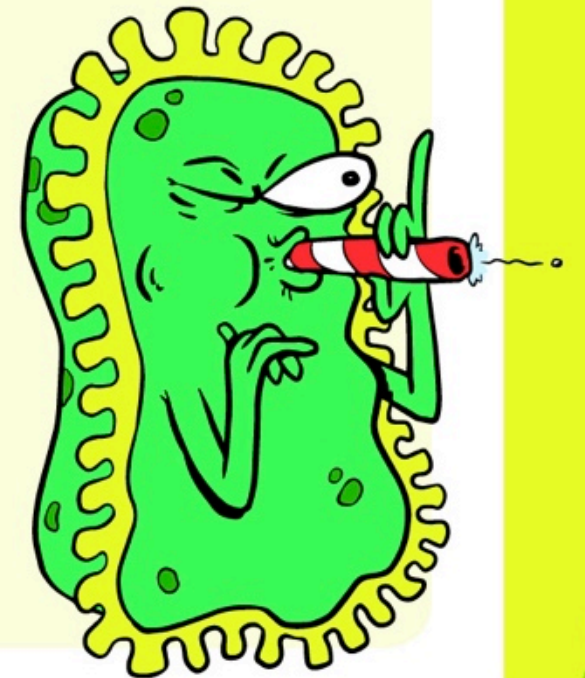


MICROTARGETETER

Microtargeting is all about the details – Your personal details, to be exact. It uses this data to segment users into smaller and smaller groups and serve them targeted content... and increasingly polarizing misinformation.

WEAKNESS

Microtargeter feeds on data and thrives in an echo chamber. Be mindful of the info you share online, and be cautious of Facebook Groups and other specialized spaces.



KNOW YOUR TROLL

20



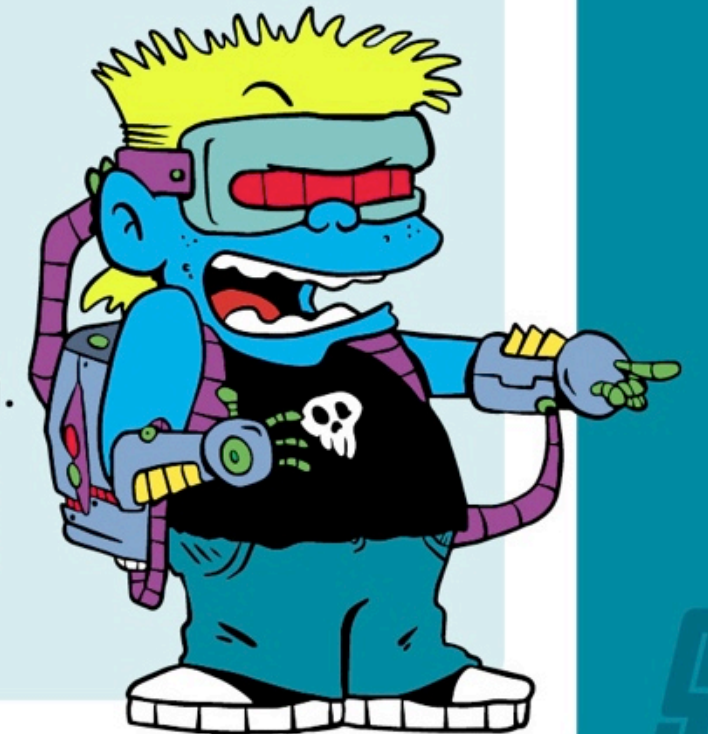
CYBERBULLY

CYBERBULLY

The internet has made life so convenient that now bullies don't even need to leave their homes to harass people. Cyberbullies can work alone or in organized campaigns that are often socially and politically motivated.

WEAKNESS

Just like their IRL counterparts, Cyberbullies are looking for a reaction. Don't give it to them. Just mute, block, and report them instead.



THANK YOU!

**For additional information, see Shots Heard
toolkit: <https://shotsheard.org/>**

Joe Smyser, PhD, MSPH
CEO, PGP
joe.smyser@publicgoodprojects.org