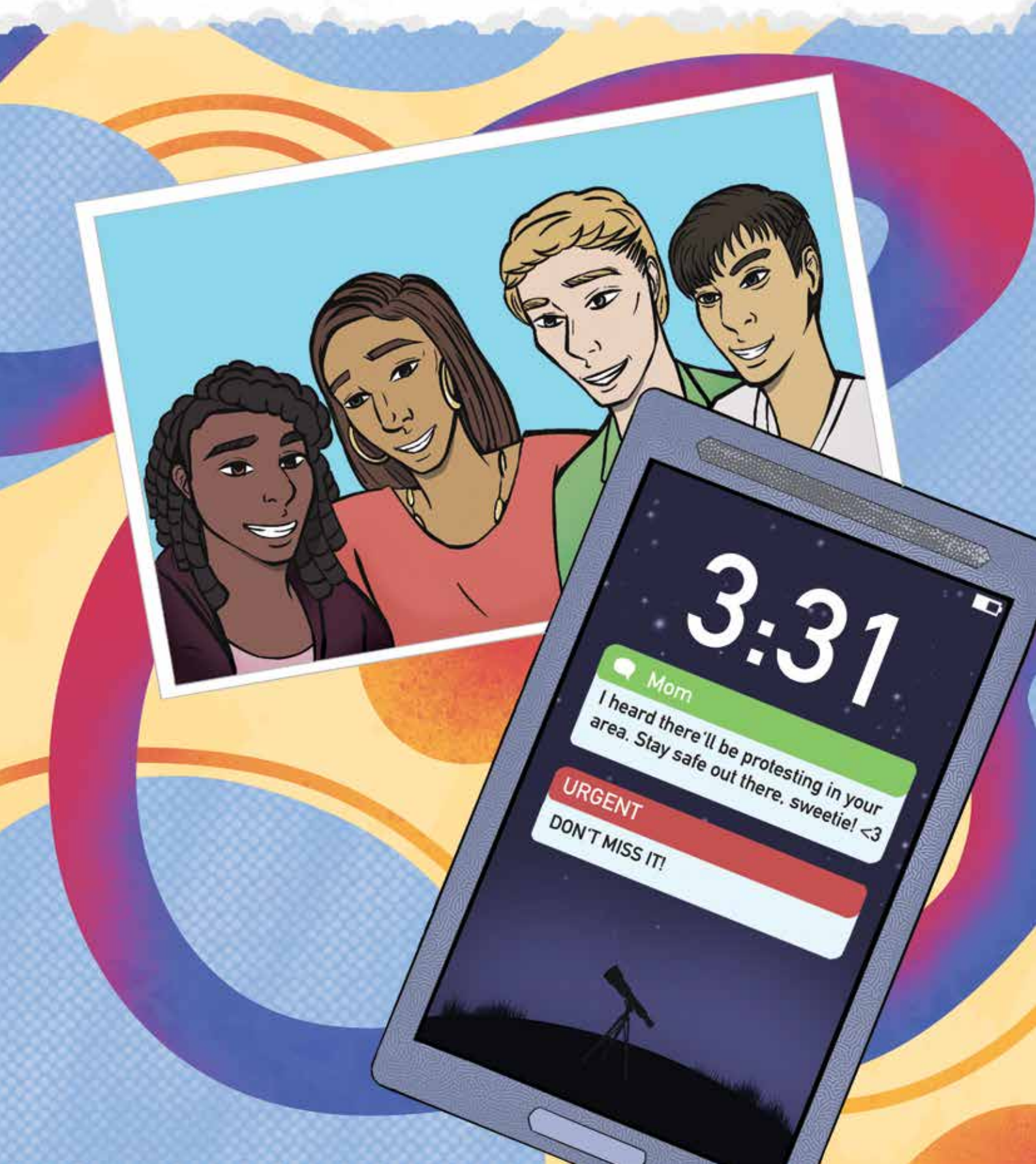
ART BY HARA LIVANI

WRITTEN BY FRANZISKA SCHRAUT

CODE OF COURAGE

A COMIC ABOUT DIGITAL SECURITY FOR ACTIVISTS



School of Arts & Creative Industries | MIMA | Teesside University

TECHNISCHE UNIVERSITÄT DARMSTADT

This comic is based on insights gathered from over 90 interviews with activists in semi-authoritarian states and countries experiencing democratic backsliding. We are immensely grateful to these activists for sharing their experiences, shedding light on the technology-facilitated violence they face, and discussing strategies they've used to protect their privacy and security.

While this comic provides general recommendations, it's crucial to emphasize that activists themselves are the true experts on their own situations. Every context is unique, and what works in one place might not be suitable in another. Risks evolve quickly, and laws—such as those targeting tools like VPNs—can change without warning. Staying informed, conducting personal threat analyses, and adapting security practices to local contexts are steps that might help in developing effective coping mechanisms. It's also important to view security holistically, recognizing that the digital and physical worlds are deeply interconnected. Online security measures are just one part of a broader approach to staying secure. Organizations such as Access Now and Front Line Defenders offer valuable resources for analyzing threats and improving digital security.

While we look forward to a future free from oppression, we remain inspired by those working tirelessly toward a more just and equitable world.

Signed: Laura Guntrum, Technical University of Darmstadt.

L. Guntrum

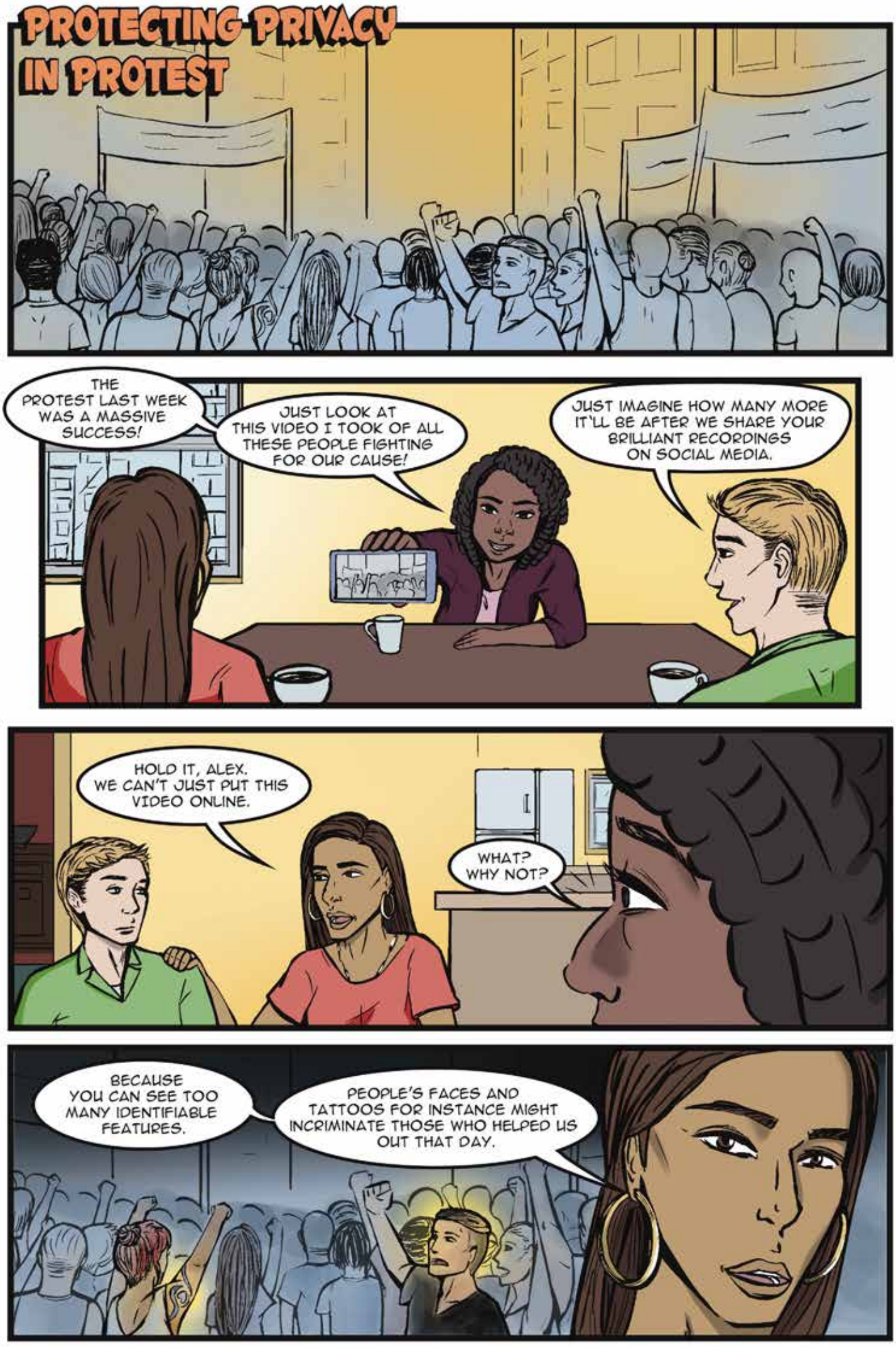
Editorial assistance: Julian Lawrence, Teesside University.

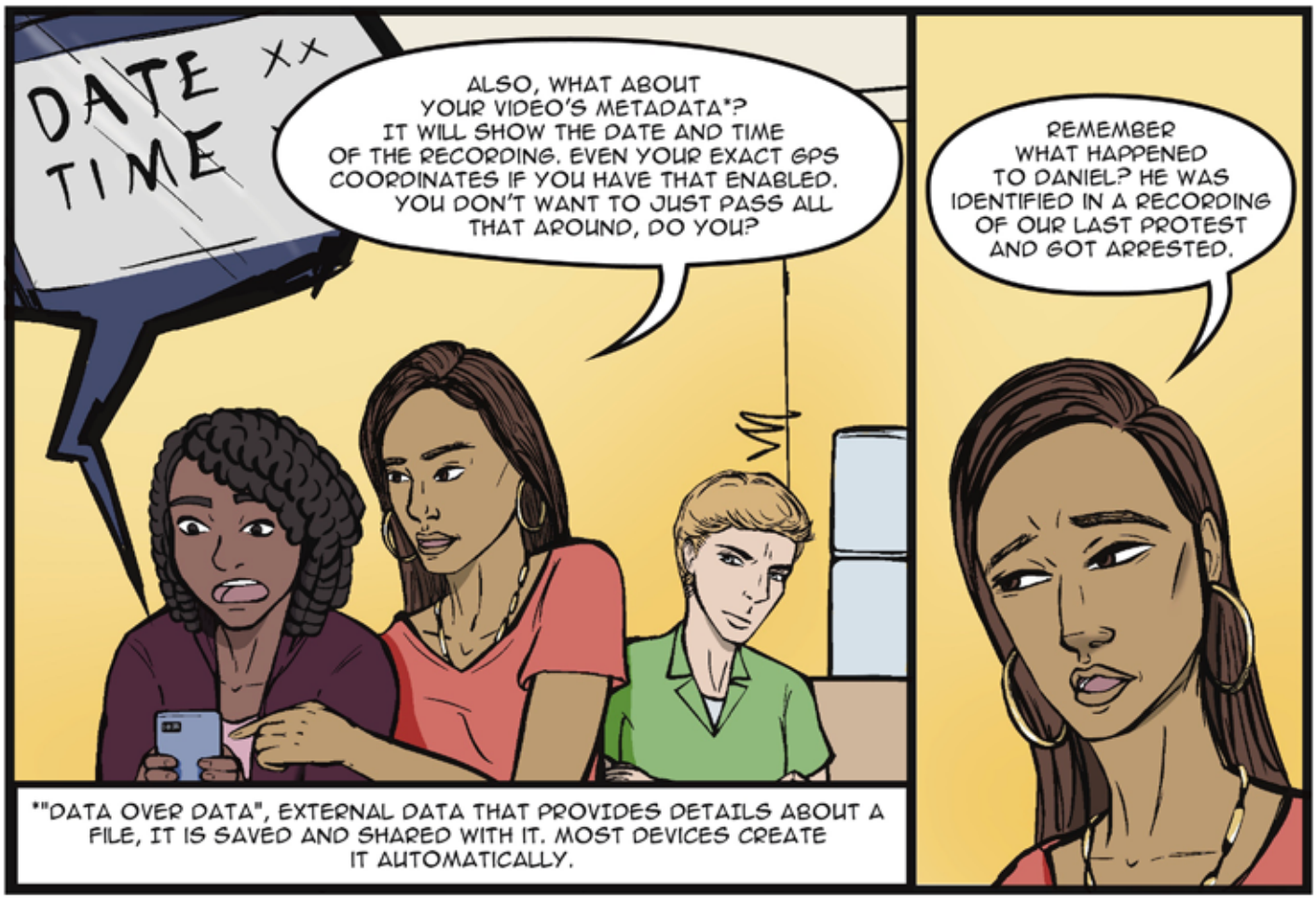
This work is licensed under a Creative Commons Attribution-Non Commercial- 4.0 International License (CC BY- NC 4.0). It was funded by the German Federal Ministry of Education and Research (BMBF) within the framework of TraCe, the Regional Research Centre on Transformations of Political Violence (01UG2203E) and by the Hessian Ministry of Higher Education, Research, Science, and the Arts as part of its joint support for the National Research Centre for Applied Cybersecurity ATHENE.

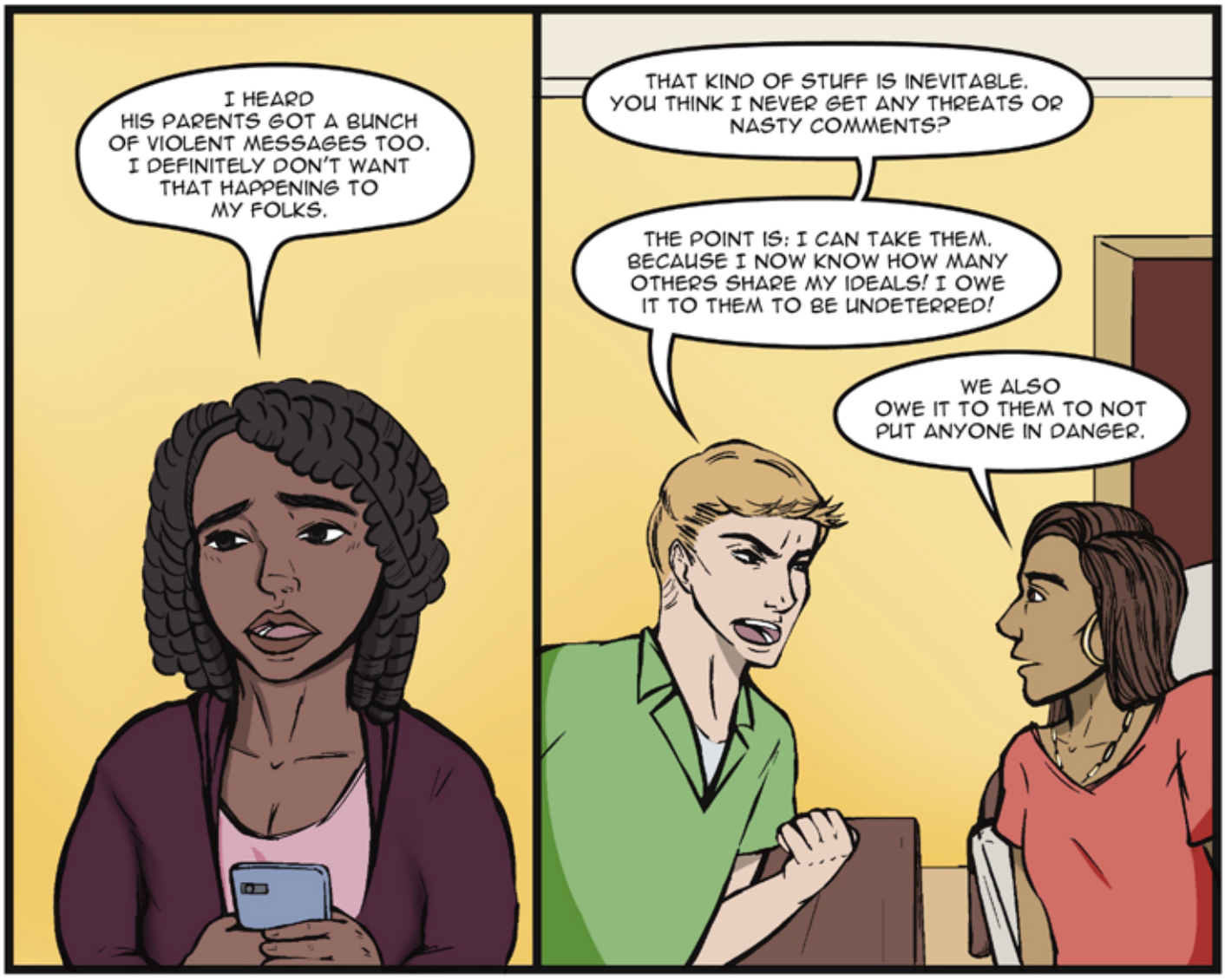
PEASEC Science and Technology for Peace and Security

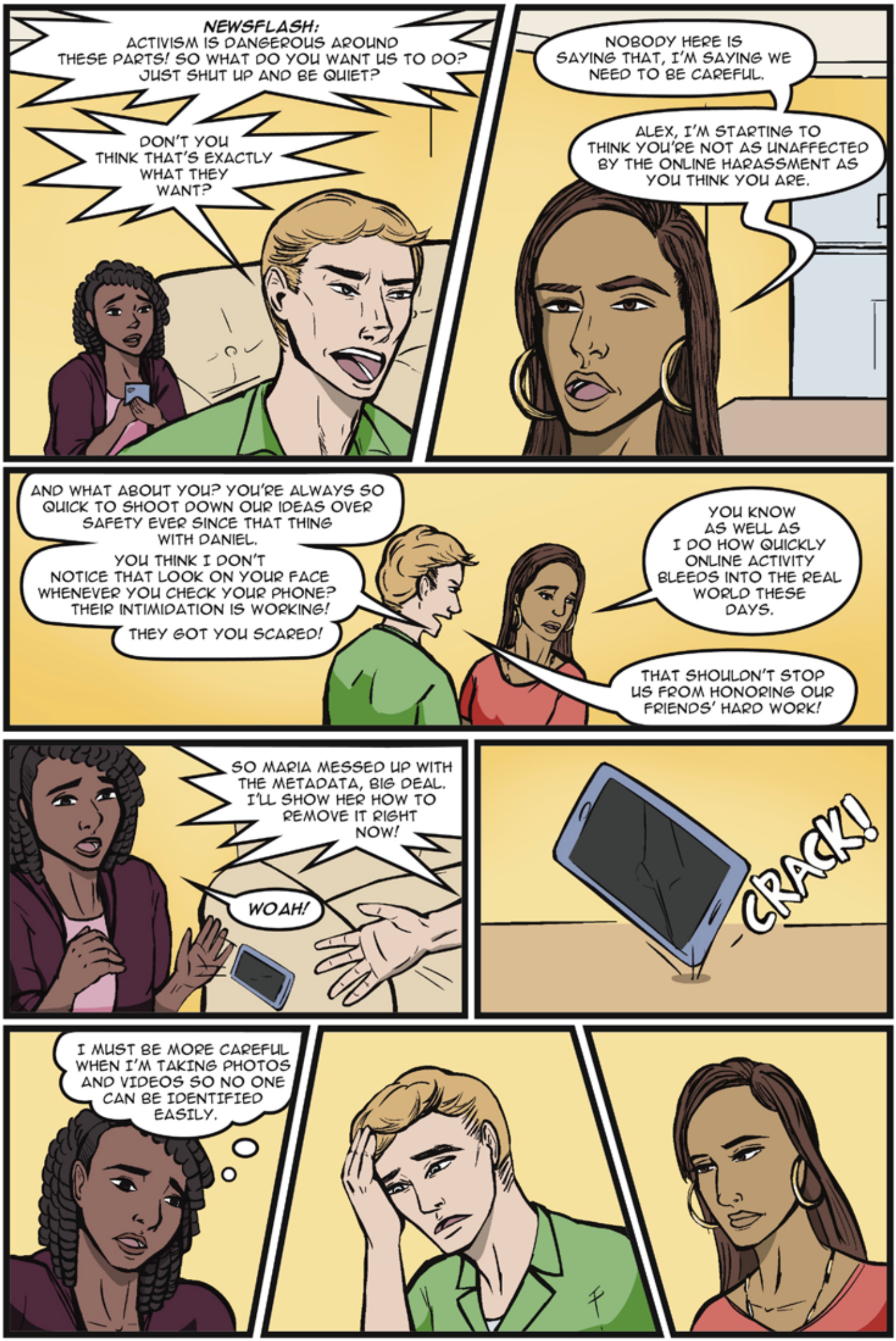
ATHENE National Research Center for Applied Cybersecurity

TraCe Research Center Transformations of Political Violence


PROTECTING PRIVACY IN PROTEST
THE PROTEST LAST WEEK WAS A MASSIVE SUCCESS!
JUST LOOK AT THIS VIDEO I TOOK OF ALL THESE PEOPLE FIGHTING FOR OUR CAUSE!
JUST IMAGINE HOW MANY MORE IT'LL BE AFTER WE SHARE YOUR BRILLIANT RECORDINGS ON SOCIAL MEDIA.
HOLD IT, ALEX. WE CAN'T JUST PUT THIS VIDEO ONLINE.
WHAT? WHY NOT?
BECAUSE YOU CAN SEE TOO MANY IDENTIFIABLE FEATURES.
PEOPLE'S FACES AND TATTOOS FOR INSTANCE MIGHT INCRIMINATE THOSE WHO HELPED US OUT THAT DAY.

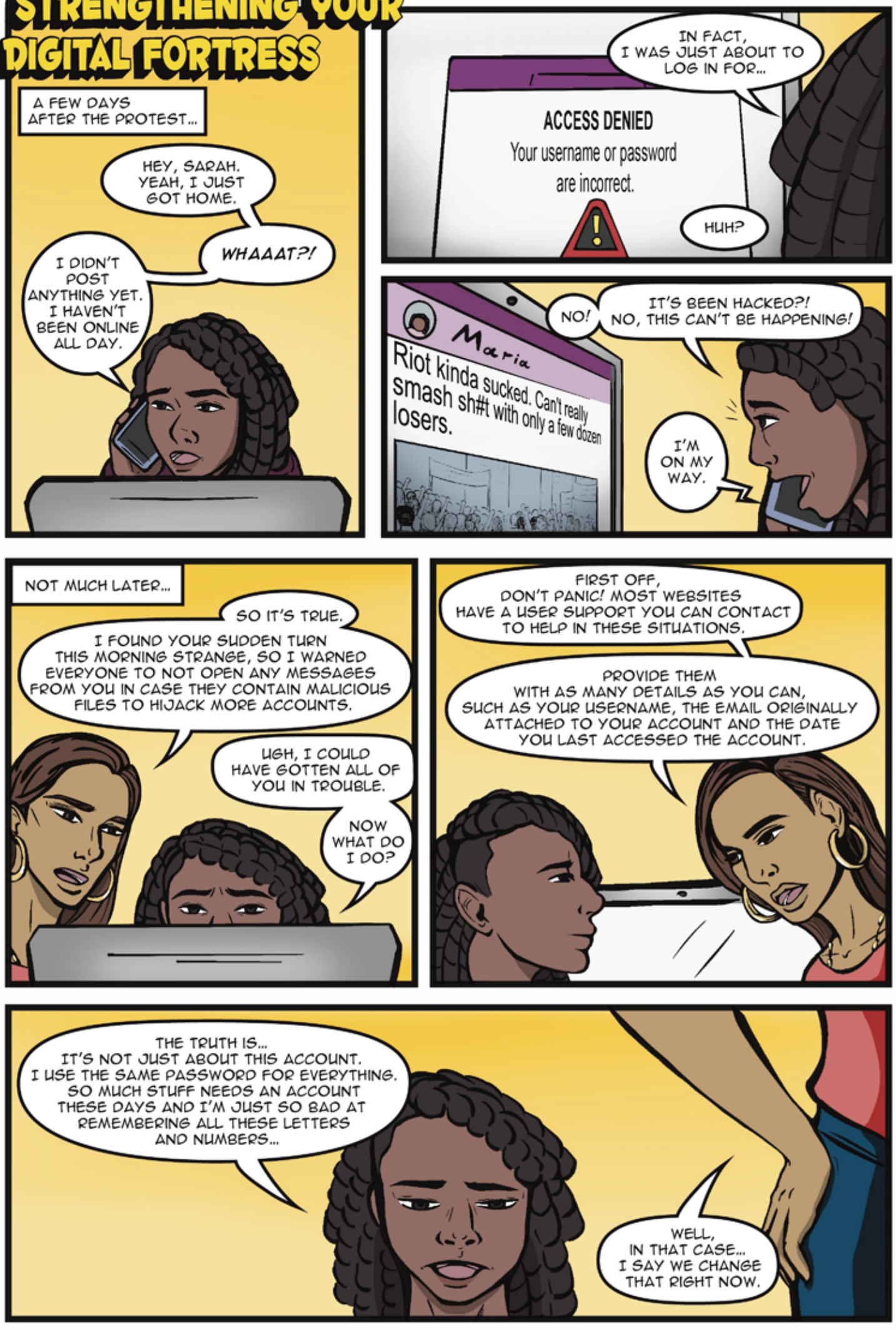

DATE
TIME
XX
ALSO, WHAT ABOUT YOUR VIDEO'S METADATA*? IT WILL SHOW THE DATE AND TIME OF THE RECORDING. EVEN YOUR EXACT GPS COORDINATES IF YOU HAVE THAT ENABLED. YOU DON'T WANT TO JUST PASS ALL THAT AROUND, DO YOU?
REMEMBER WHAT HAPPENED TO DANIEL? HE WAS IDENTIFIED IN A RECORDING OF OUR LAST PROTEST AND GOT ARRESTED.
*"DATA OVER DATA", EXTERNAL DATA THAT PROVIDES DETAILS ABOUT A FILE, IT IS SAVED AND SHARED WITH IT. MOST DEVICES CREATE IT AUTOMATICALLY.


I HEARD HIS PARENTS GOT A BUNCH OF VIOLENT MESSAGES TOO. I DEFINITELY DON'T WANT THAT HAPPENING TO MY FOLKS.
THAT KIND OF STUFF IS INEVITABLE. YOU THINK I NEVER GET ANY THREATS OR NASTY COMMENTS?
THE POINT IS: I CAN TAKE THEM. BECAUSE I NOW KNOW HOW MANY OTHERS SHARE MY IDEALS! I OWE IT TO THEM TO BE UNDETERRED!
WE ALSO OWE IT TO THEM TO NOT PUT ANYONE IN DANGER.

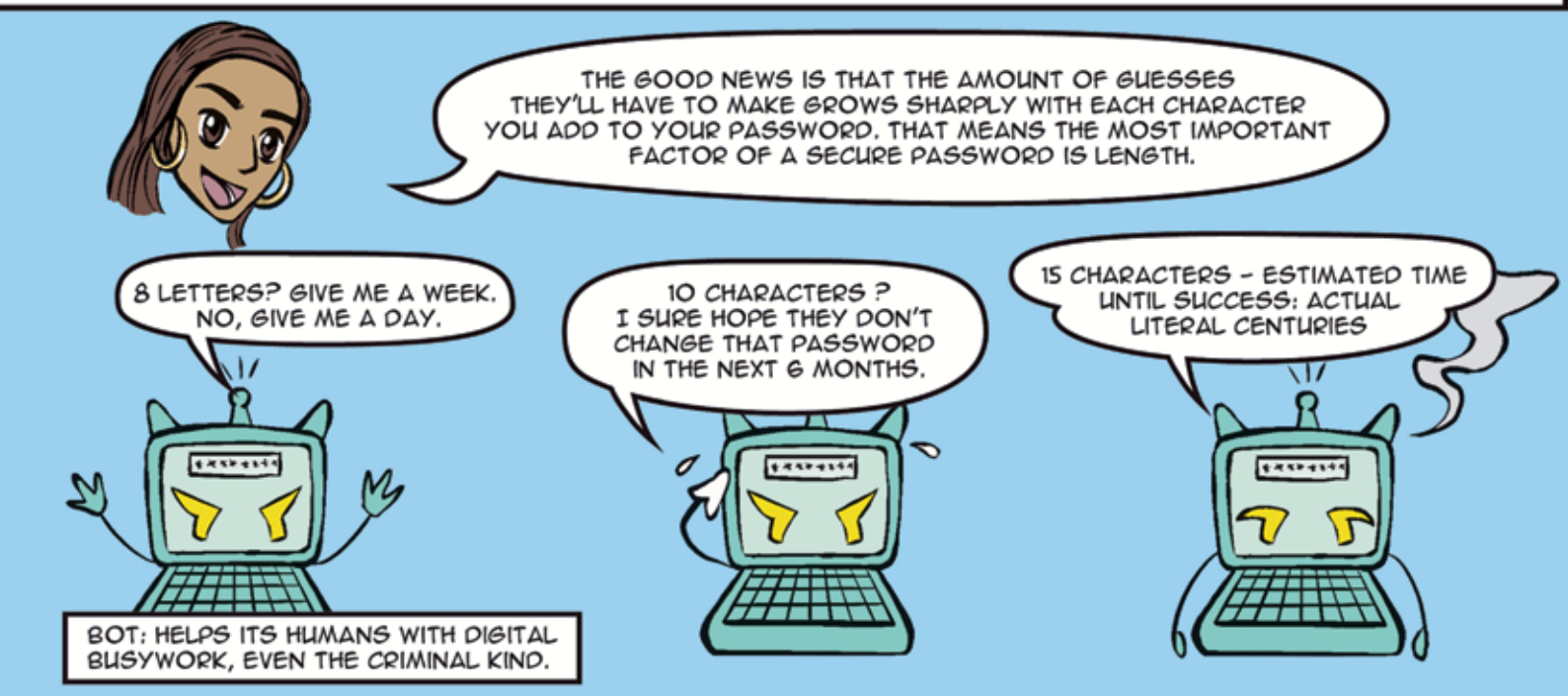

NEWSFLASH:
ACTIVISM IS DANGEROUS AROUND THESE PARTS! SO WHAT DO YOU WANT US TO DO? JUST SHUT UP AND BE QUIET?
DON'T YOU THINK THAT'S EXACTLY WHAT THEY WANT?
NOBODY HERE IS SAYING THAT, I'M SAYING WE NEED TO BE CAREFUL.
ALEX, I'M STARTING TO THINK YOU'RE NOT AS UNAFFECTED BY THE ONLINE HARASSMENT AS YOU THINK YOU ARE.
AND WHAT ABOUT YOU? YOU'RE ALWAYS SO QUICK TO SHOOT DOWN OUR IDEAS OVER SAFETY EVER SINCE THAT THING WITH DANIEL.
YOU THINK I DON'T NOTICE THAT LOOK ON YOUR FACE WHENEVER YOU CHECK YOUR PHONE? THEIR INTIMIDATION IS WORKING!
THEY GOT YOU SCARED!
YOU KNOW AS WELL AS I DO HOW QUICKLY ONLINE ACTIVITY BLEEDS INTO THE REAL WORLD THESE DAYS.
THAT SHOULDN'T STOP US FROM HONORING OUR FRIENDS' HARD WORK!
SO MARIA MESSED UP WITH THE METADATA, BIG DEAL. I'LL SHOW HER HOW TO REMOVE IT RIGHT NOW!
WOAH!
CRACK!
I MUST BE MORE CAREFUL WHEN I'M TAKING PHOTOS AND VIDEOS SO NO ONE CAN BE IDENTIFIED EASILY.

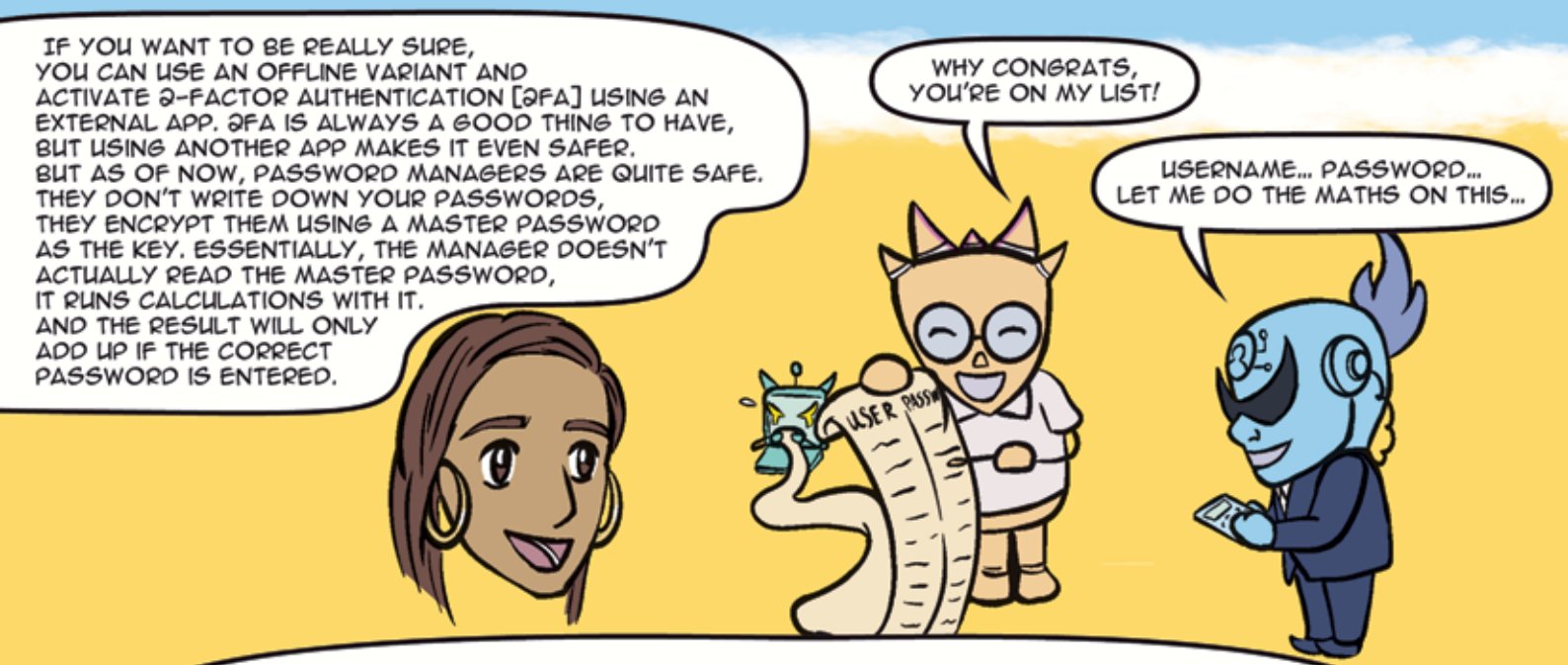

MARIA, I'M SO SORRY. I'M SUCH AN IDIOT. YOU DID GREAT OUT THERE, I JUST WANTED TO...
IT'S OKAY. I GUESS WE'RE ALL A BIT MORE ON EDGE THAN WE REALIZED.
WE SHOULD ALL CALM DOWN. I KNOW A GREAT PLACE FOR COFFEE. LET'S TAKE OUR MIND OFF OF THINGS FOR A BIT.WE CAN STILL LOOK INTO ADJUSTING THE VIDEO TO OBSCURE FACES AND REMOVE THE ORIGINAL METADATA FOR THE FUTURE.
SOUNDS GOOD. I'LL JUST DISABLE GPS ACCESS ON MY CAMERA REAL QUICK.
11:00
You little b
better watch your back.
BREATHE, MARIA. KEEP A COOL HEAD. IT'S JUST ANOTHER MESSAGE.
CLICK!
THE INTERNET IS UNPREDICTABLE AND NEVER FORGETS. BE MINDFUL OF WHAT YOU UPLOAD.
AND YET... PHYSICAL VIOLENCE... DIGITAL VIOLENCE... THEY'RE NOT SO FAR APART, ARE THEY?
ONCE SOMETHING IS UPLOADED TO THE INTERNET, IT'S CHALLENGING TO FULLY REMOVE BECAUSE COPIES ARE OFTEN STORED ON VARIOUS SERVERS AND CAN BE ACCESSED OR SHARED BY OTHERS INDEFINITELY.

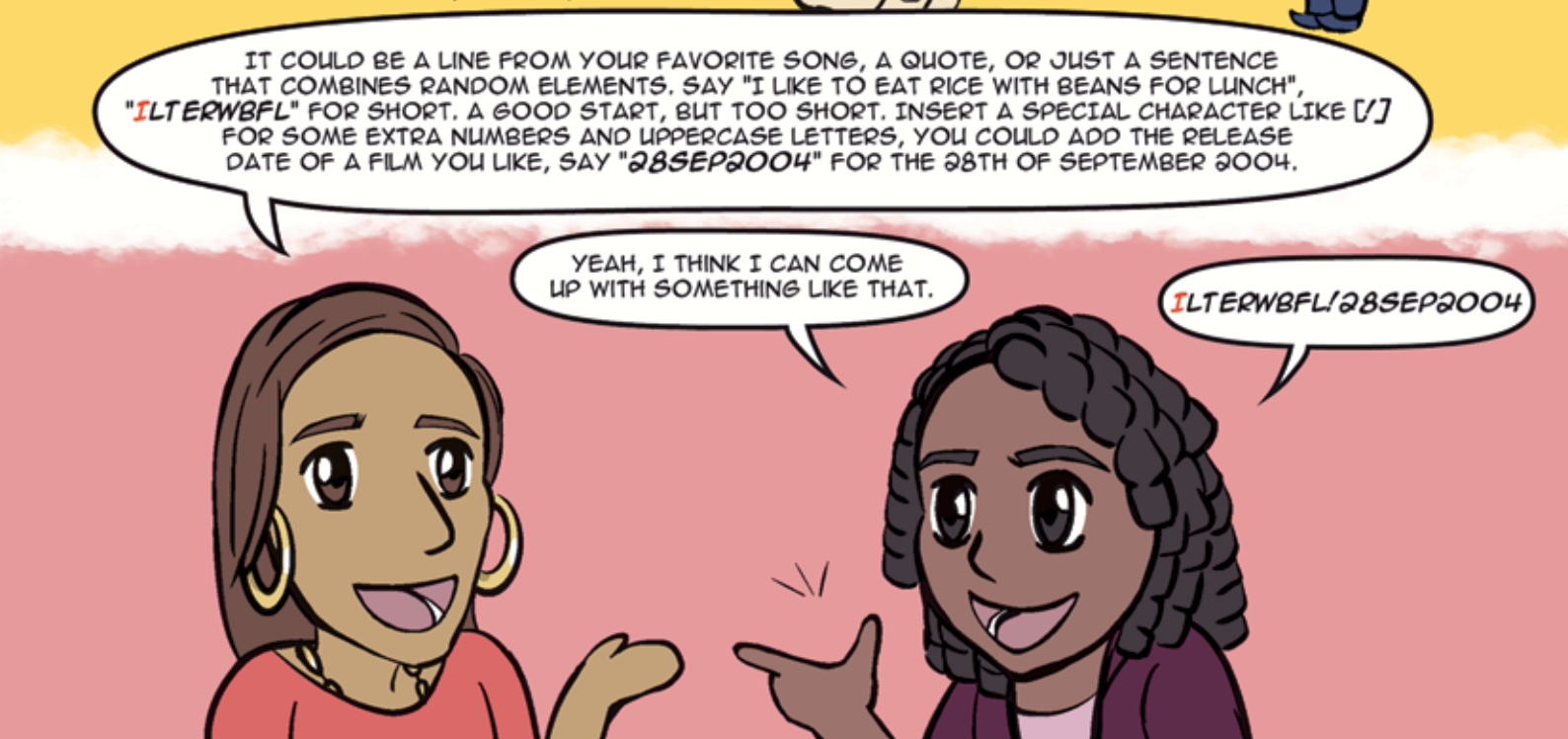
STRENGTHENING YOUR DIGITAL FORTRESS

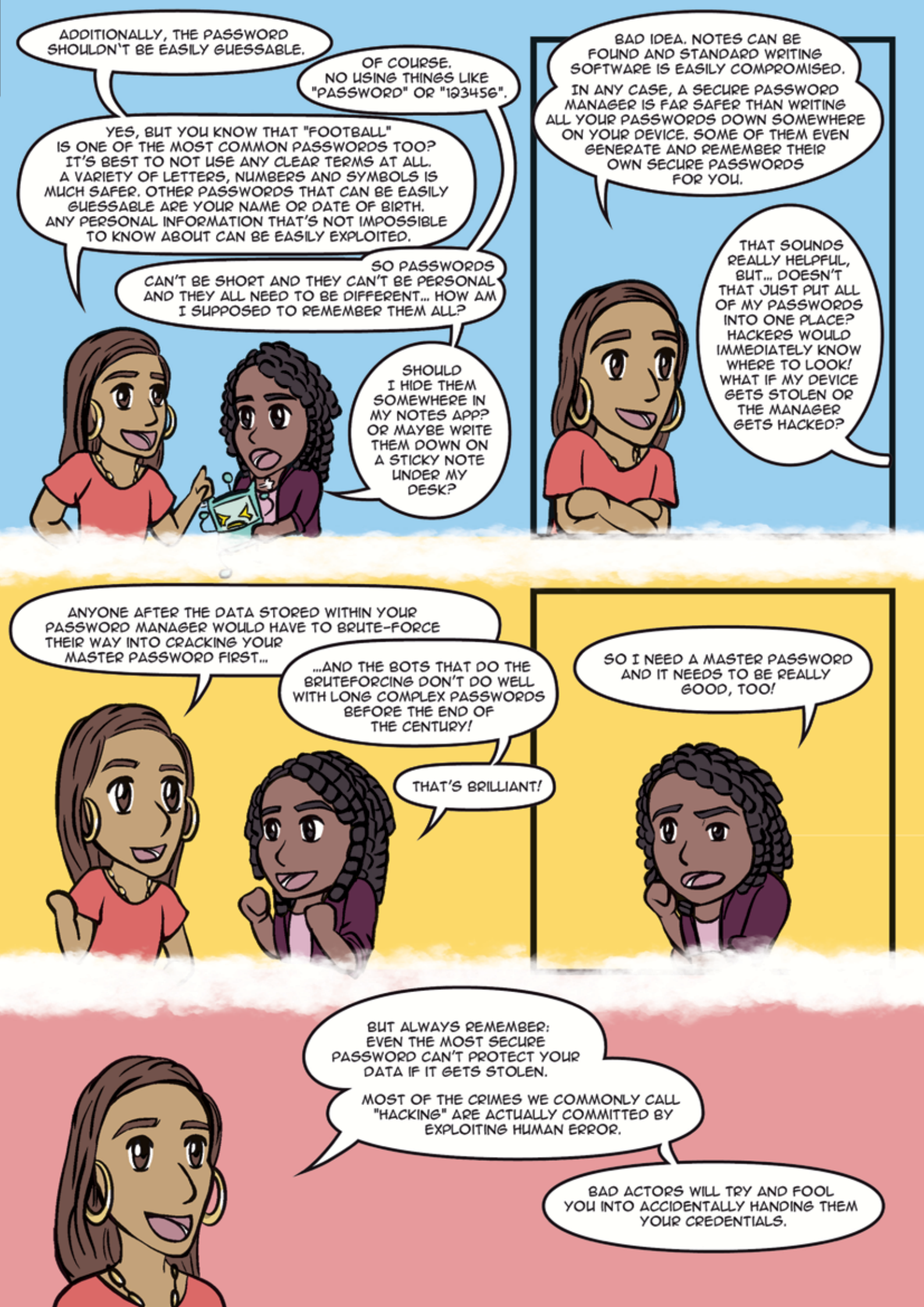


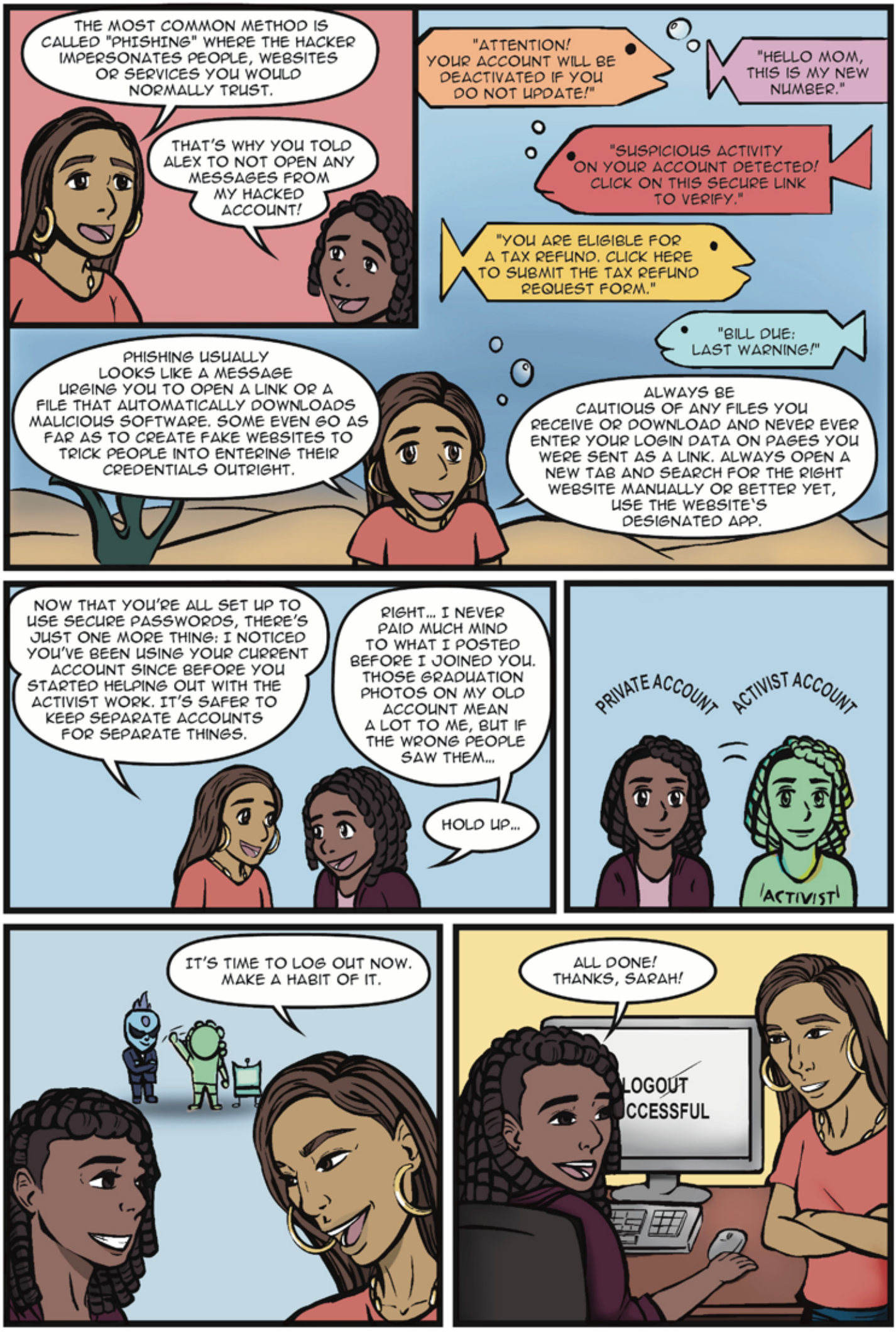
THE INTERNET IS AN INCREDIBLE TOOL, BUT KEEPING YOUR PERSONAL DATA FROM BEING ACCESSED BY THE WRONG PEOPLE IS KEY TO NAVIGATING IT SAFELY. FOR PASSWORDS, THERE ARE A FEW THINGS TO CONSIDER.A LOT OF TARGETED HACKS USE BOTS TO GUESS PASSWORDS THROUGH BRUTE FORCE. THESE BOTS ARE AUTOMATED COMPUTER PROGRAMS THAT CAN TRY HUNDREDS OF PASSWORDS PER MINUTE UNTIL THEY GET IT RIGHT.








ADDITIONALLY, THE PASSWORD SHOULDN'T BE EASILY GUESSABLE.
OF COURSE. NO USING THINGS LIKE "PASSWORD" OR "123456".
YES, BUT YOU KNOW THAT "FOOTBALL" IS ONE OF THE MOST COMMON PASSWORDS TOO? IT'S BEST TO NOT USE ANY CLEAR TERMS AT ALL. A VARIETY OF LETTERS, NUMBERS AND SYMBOLS IS MUCH SAFER. OTHER PASSWORDS THAT CAN BE EASILY GUESSABLE ARE YOUR NAME OR DATE OF BIRTH. ANY PERSONAL INFORMATION THAT'S NOT IMPOSSIBLE TO KNOW ABOUT CAN BE EASILY EXPLOITED.
SO PASSWORDS CAN'T BE SHORT AND THEY CAN'T BE PERSONAL AND THEY ALL NEED TO BE DIFFERENT... HOW AM I SUPPOSED TO REMEMBER THEM ALL?
SHOULD I HIDE THEM SOMEWHERE IN MY NOTES APP? OR MAYBE WRITE THEM DOWN ON A STICKY NOTE UNDER MY DESK?
BAD IDEA. NOTES CAN BE FOUND AND STANDARD WRITING SOFTWARE IS EASILY COMPROMISED.
IN ANY CASE, A SECURE PASSWORD MANAGER IS FAR SAFER THAN WRITING ALL YOUR PASSWORDS DOWN SOMEWHERE ON YOUR DEVICE. SOME OF THEM EVEN GENERATE AND REMEMBER THEIR OWN SECURE PASSWORDS FOR YOU.
THAT SOUNDS REALLY HELPFUL, BUT... DOESN'T THAT JUST PUT ALL OF MY PASSWORDS INTO ONE PLACE? HACKERS WOULD IMMEDIATELY KNOW WHERE TO LOOK! WHAT IF MY DEVICE GETS STOLEN OR THE MANAGER GETS HACKED?
ANYONE AFTER THE DATA STORED WITHIN YOUR PASSWORD MANAGER WOULD HAVE TO BRUTE-FORCE THEIR WAY INTO CRACKING YOUR MASTER PASSWORD FIRST...
...AND THE BOTS THAT DO THE BRUTEFORCING DON'T DO WELL WITH LONG COMPLEX PASSWORDS BEFORE THE END OF THE CENTURY!
THAT'S BRILLIANT!
SO I NEED A MASTER PASSWORD AND IT NEEDS TO BE REALLY GOOD, TOO!
BUT ALWAYS REMEMBER: EVEN THE MOST SECURE PASSWORD CAN'T PROTECT YOUR DATA IF IT GETS STOLEN.
MOST OF THE CRIMES WE COMMONLY CALL "HACKING" ARE ACTUALLY COMMITTED BY EXPLOITING HUMAN ERROR.
BAD ACTORS WILL TRY AND FOOL YOU INTO ACCIDENTALLY HANDING THEM YOUR CREDENTIALS.


THE MOST COMMON METHOD IS CALLED "PHISHING" WHERE THE HACKER IMPERSONATES PEOPLE, WEBSITES OR SERVICES YOU WOULD NORMALLY TRUST.
THAT'S WHY YOU TOLD ALEX TO NOT OPEN ANY MESSAGES FROM MY HACKED ACCOUNT!
"ATTENTION! YOUR ACCOUNT WILL BE DEACTIVATED IF YOU DO NOT UPDATE!"
"HELLO MOM, THIS IS MY NEW NUMBER."
"SUSPICIOUS ACTIVITY ON YOUR ACCOUNT DETECTED! CLICK ON THIS SECURE LINK TO VERIFY."
"YOU ARE ELIGIBLE FOR A TAX REFUND. CLICK HERE TO SUBMIT THE TAX REFUND REQUEST FORM."
"BILL DUE: LAST WARNING!"
PHISHING USUALLY LOOKS LIKE A MESSAGE URGING YOU TO OPEN A LINK OR A FILE THAT AUTOMATICALLY DOWNLOADS MALICIOUS SOFTWARE. SOME EVEN GO AS FAR AS TO CREATE FAKE WEBSITES TO TRICK PEOPLE INTO ENTERING THEIR CREDENTIALS OUTRIGHT.
ALWAYS BE CAUTIOUS OF ANY FILES YOU RECEIVE OR DOWNLOAD AND NEVER EVER ENTER YOUR LOGIN DATA ON PAGES YOU WERE SENT AS A LINK. ALWAYS OPEN A NEW TAB AND SEARCH FOR THE RIGHT WEBSITE MANUALLY OR BETTER YET, USE THE WEBSITE'S DESIGNATED APP.
NOW THAT YOU'RE ALL SET UP TO USE SECURE PASSWORDS, THERE'S JUST ONE MORE THING: I NOTICED YOU'VE BEEN USING YOUR CURRENT ACCOUNT SINCE BEFORE YOU STARTED HELPING OUT WITH THE ACTIVIST WORK. IT'S SAFER TO KEEP SEPARATE ACCOUNTS FOR SEPARATE THINGS.
RIGHT... I NEVER PAID MUCH MIND TO WHAT I POSTED BEFORE I JOINED YOU. THOSE GRADUATION PHOTOS ON MY OLD ACCOUNT MEAN A LOT TO ME, BUT IF THE WRONG PEOPLE SAW THEM...
HOLD UP...
PRIVATE ACCOUNT
ACTIVIST ACCOUNT
!ACTIVIST!
IT'S TIME TO LOG OUT NOW. MAKE A HABIT OF IT.
ALL DONE! THANKS, SARAH!
LOGOUT
CCESSFUL


STAYING SECURE DURING DEVICE INSPECTIONS
YOU KNOW, YOU REALLY DIDN'T HAVE TO BUY ME A NEW PHONE OVER THAT ONE SCREEN CRACK, ALEX.
IT'S THE LEAST I COULD DO. BESIDES, I KNOW WHERE TO GET THE BEST DEALS.
HALT!
WE'RE CONDUCTING INSPECTIONS OF COMMUNICATION DEVICES. I NEED TO TAKE A LOOK AT YOUR PHONES IF YOU PLEASE.
MY OLD PHONE HAD A BIT OF AN ACCIDENT.
SORRY.
CLICK
Welcome
I TAKE IT YOUR PHONE DIDN'T HAVE ANY ACCIDENTS?
OF COURSE NOT, GEEZ.


I SEE YOU'RE LOGGED OUT OF ALL OF YOUR SOCIAL MEDIA.
YEAH. ISN'T THAT HOW YOU PREVENT BEING HACKED THESE DAYS?
LOG INTO THIS ONE.
HERE WE GO.
Alex
HM. THANK YOU FOR YOUR COOPERATION.

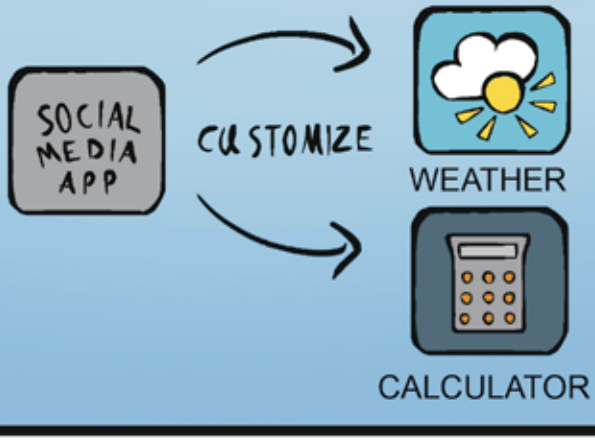
YOU WANT TO ENABLE DEVICE ENCRYPTION AND SELECT "PIN CODE". DON'T USE THE BIOMETRIC FEATURES. THAT MEANS YOU CAN'T UNLOCK YOUR PHONE WITH YOUR FACE OR YOUR FINGERPRINT, BUT NEITHER CAN ANYONE ELSE.

DEVICE ENCRYPTION

PIN CODE	ON
FACIAL CODE	OFF
FINGERPRINT ID	OFF

AN ADVERSARY CAN FORCE AN ACTIVIST TO UNLOCK THEIR DEVICE BY PHYSICALLY USING THEIR FINGERPRINTOR POSITIONING THEIR FACE IN FRONT OF A CAMERA. THIS IS MUCH HARDER WITH A PASSCODE, AS INDIVIDUALS CAN CLAIM THEY HAVE FORGOTTEN IT OR REFUSE TO DISCLOSE IT.

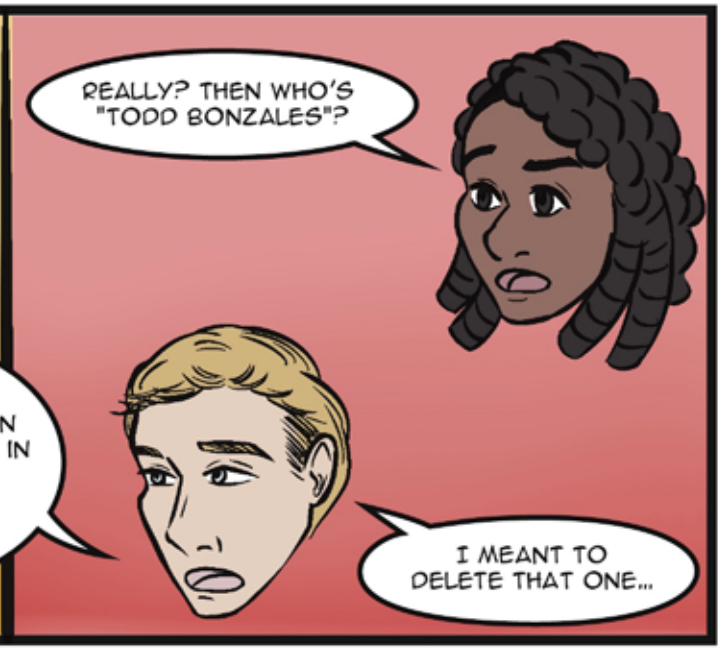
SOME APPS LET YOU CHANGE THE ICONS AND NAMES ON YOUR HOME SCREEN. APPS THAT HAVE A CERTAIN REPUTATION GET A LITTLE MAKEOVER.

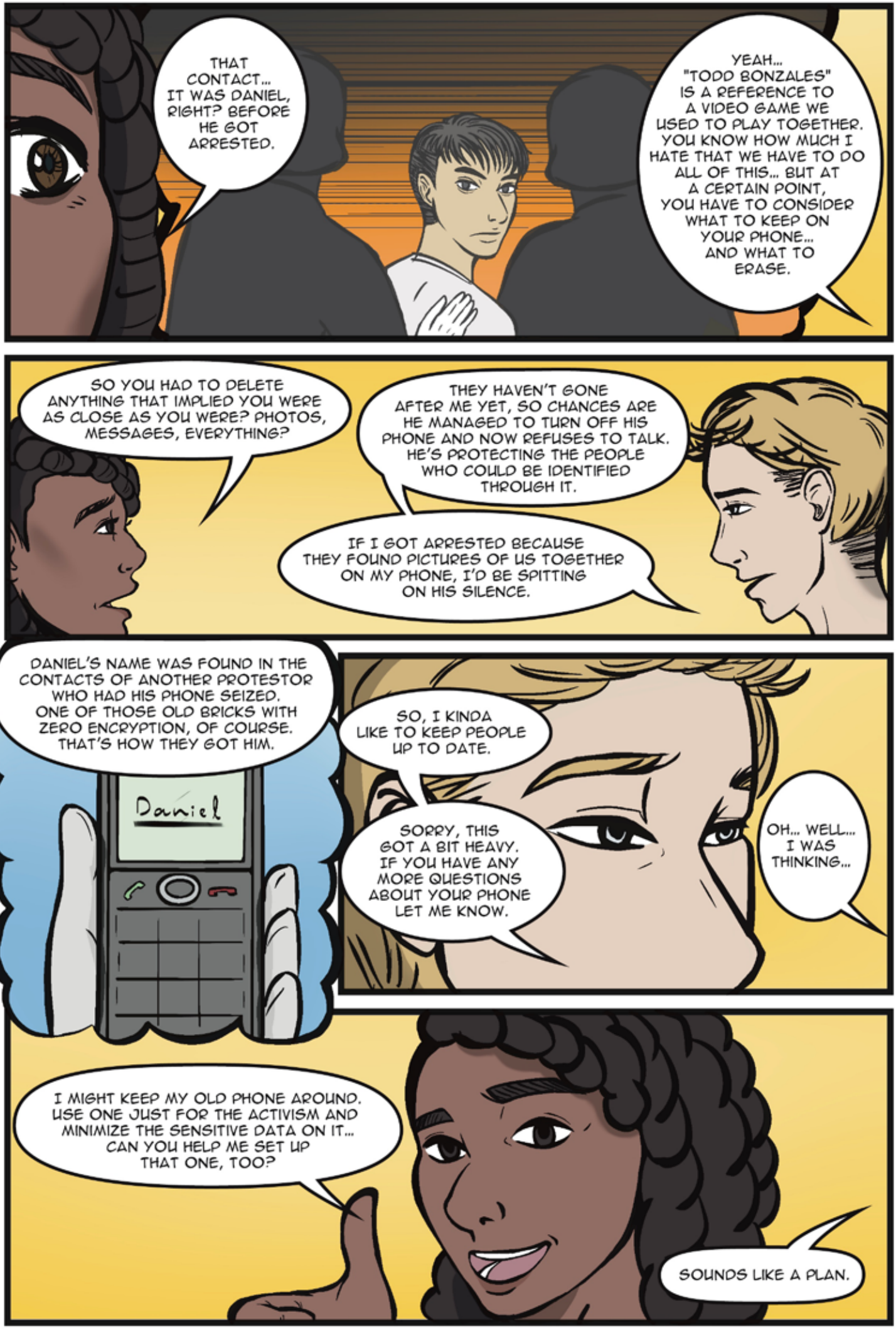


CONTACTS

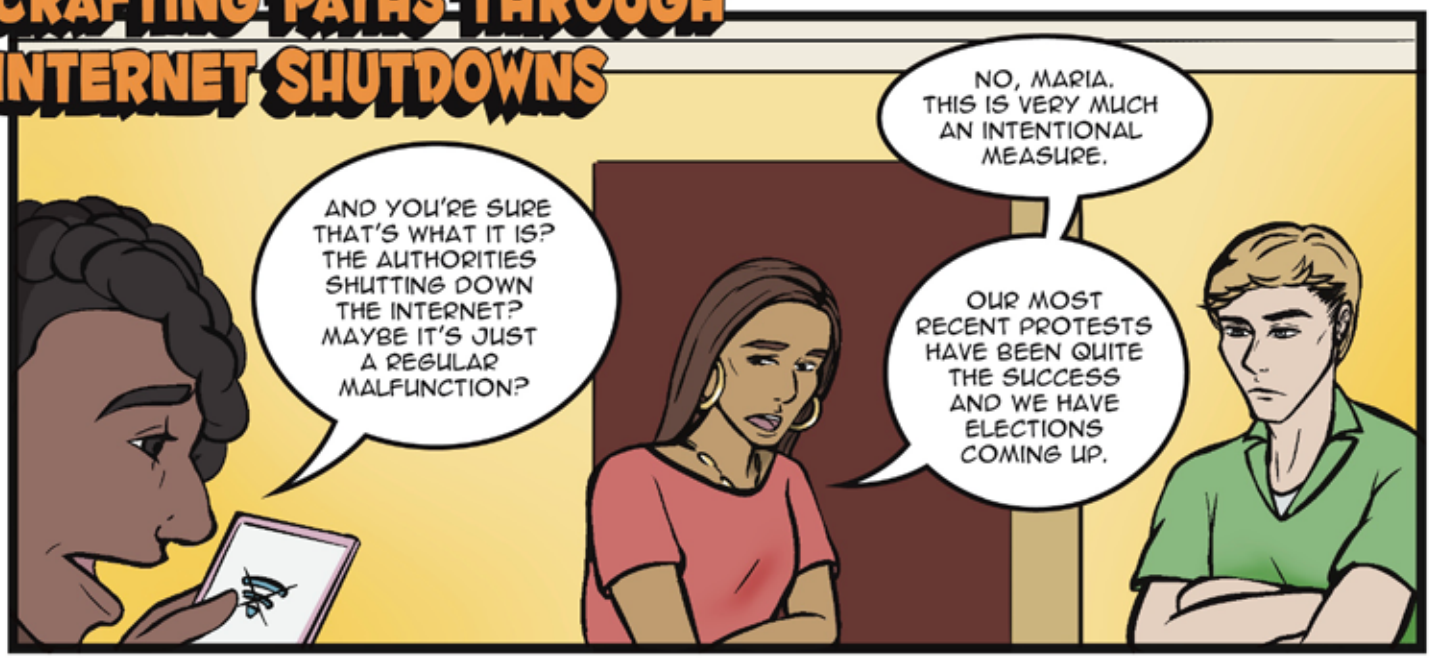
CHARLIE MARTINEZ

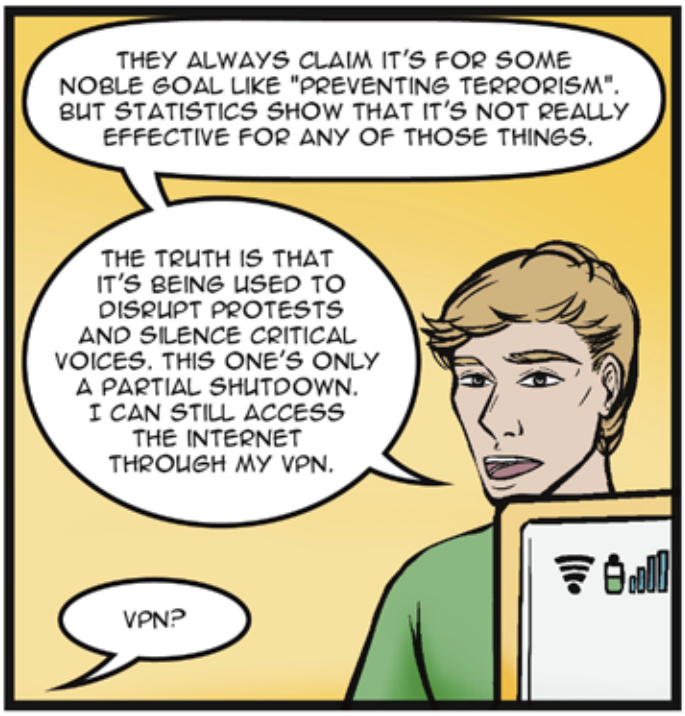
TODD BONZALES

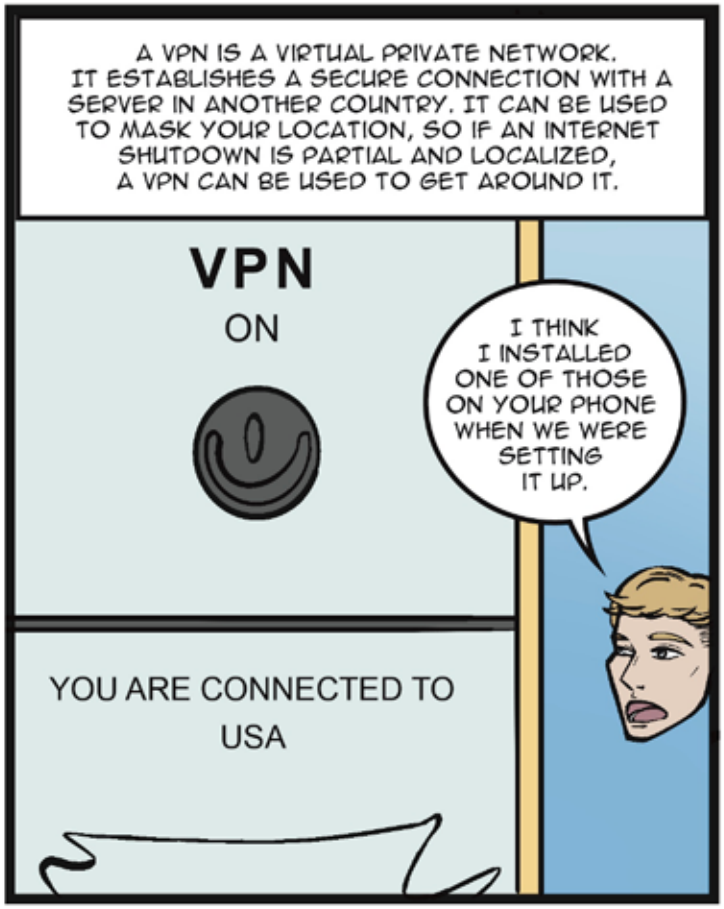


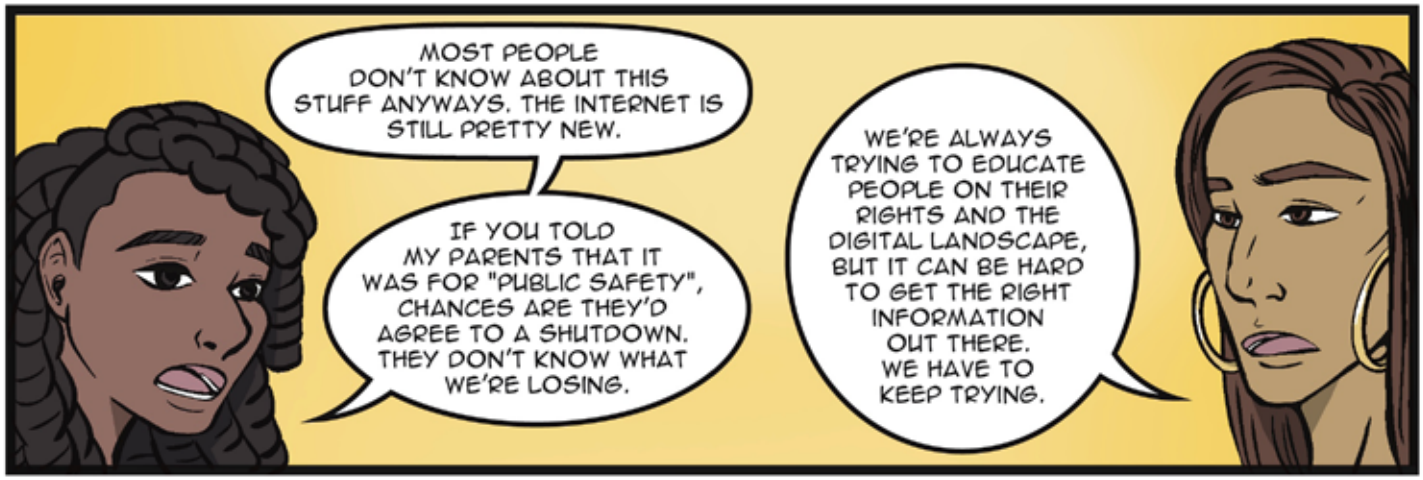

THAT CONTACT... IT WAS DANIEL, RIGHT? BEFORE HE GOT ARRESTED.
YEAH... "TODD BONZALES" IS A REFERENCE TO A VIDEO GAME WE USED TO PLAY TOGETHER. YOU KNOW HOW MUCH I HATE THAT WE HAVE TO DO ALL OF THIS... BUT AT A CERTAIN POINT, YOU HAVE TO CONSIDER WHAT TO KEEP ON YOUR PHONE... AND WHAT TO ERASE.
SO YOU HAD TO DELETE ANYTHING THAT IMPLIED YOU WERE AS CLOSE AS YOU WERE? PHOTOS, MESSAGES, EVERYTHING?
THEY HAVEN'T GONE AFTER ME YET, SO CHANCES ARE HE MANAGED TO TURN OFF HIS PHONE AND NOW REFUSES TO TALK. HE'S PROTECTING THE PEOPLE WHO COULD BE IDENTIFIED THROUGH IT.
IF I GOT ARRESTED BECAUSE THEY FOUND PICTURES OF US TOGETHER ON MY PHONE, I'D BE SPITTING ON HIS SILENCE.
DANIEL'S NAME WAS FOUND IN THE CONTACTS OF ANOTHER PROTESTOR WHO HAD HIS PHONE SEIZED. ONE OF THOSE OLD BRICKS WITH ZERO ENCRYPTION, OF COURSE. THAT'S HOW THEY GOT HIM.
Daniel
SO, I KINDA LIKE TO KEEP PEOPLE UP TO DATE.
SORRY, THIS GOT A BIT HEAVY. IF YOU HAVE ANY MORE QUESTIONS ABOUT YOUR PHONE LET ME KNOW.
OH... WELL... I WAS THINKING...
I MIGHT KEEP MY OLD PHONE AROUND. USE ONE JUST FOR THE ACTIVISM AND MINIMIZE THE SENSITIVE DATA ON IT... CAN YOU HELP ME SET UP THAT ONE, TOO?
SOUNDS LIKE A PLAN.

CRAFTING PATHS THROUGH INTERNET SHUTDOWNS

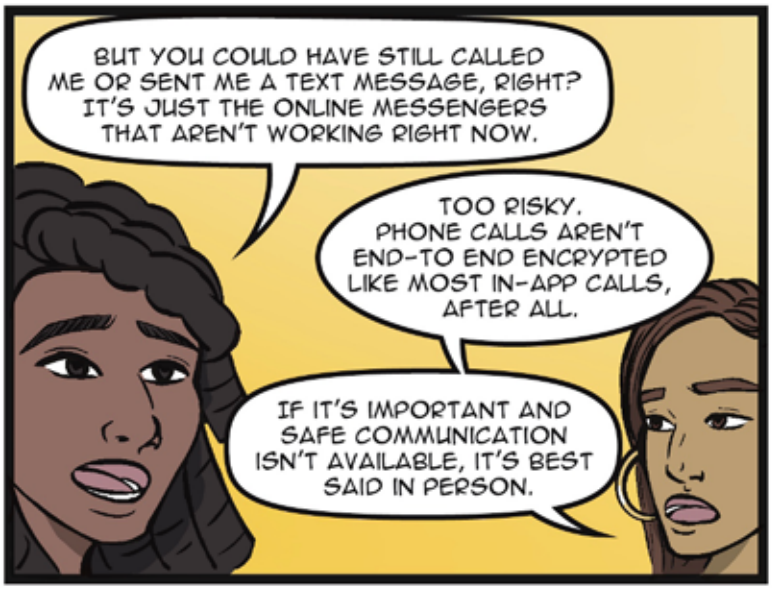


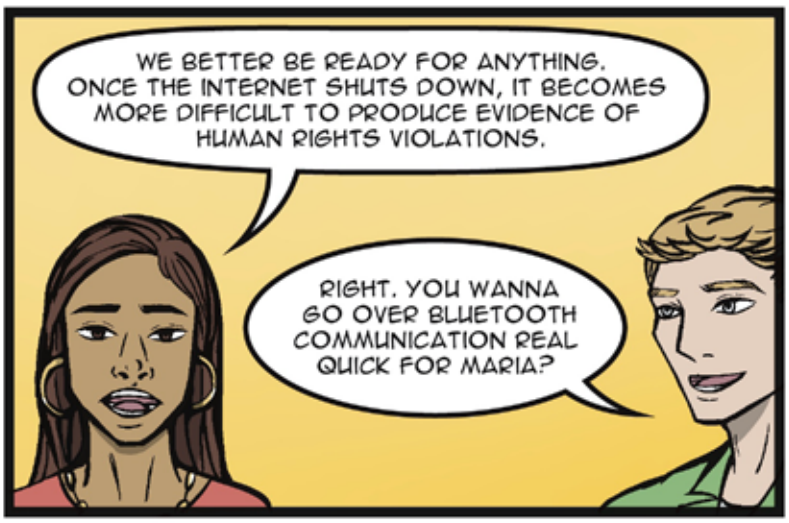




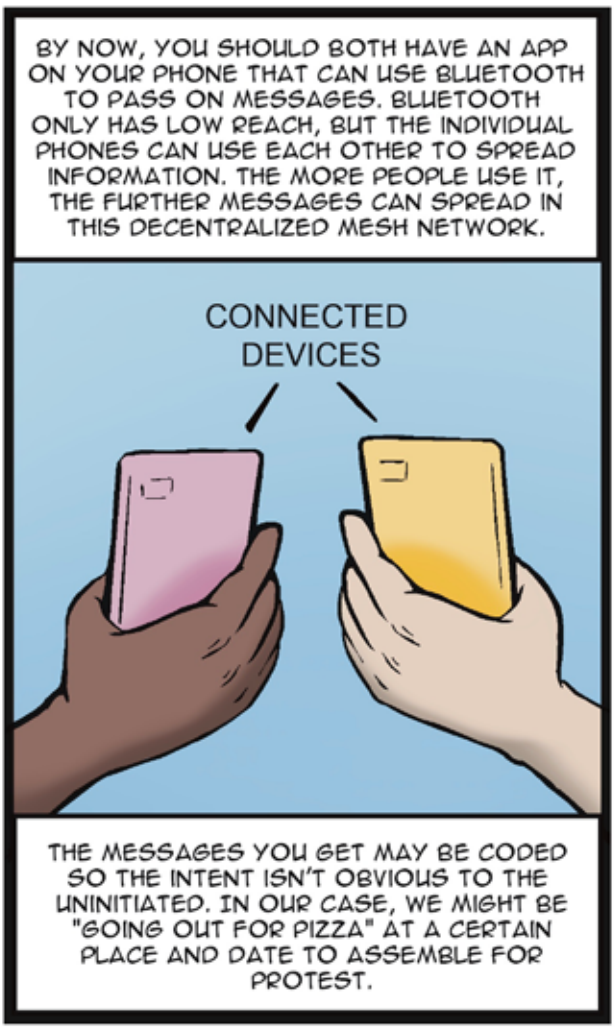

MOST PEOPLE DON'T KNOW ABOUT THIS STUFF ANYWAYS. THE INTERNET IS STILL PRETTY NEW.
IF YOU TOLD MY PARENTS THAT IT WAS FOR "PUBLIC SAFETY", CHANCES ARE THEY'D AGREE TO A SHUTDOWN. THEY DON'T KNOW WHAT WE'RE LOSING.
WE'RE ALWAYS TRYING TO EDUCATE PEOPLE ON THEIR RIGHTS AND THE DIGITAL LANDSCAPE, BUT IT CAN BE HARD TO GET THE RIGHT INFORMATION OUT THERE. WE HAVE TO KEEP TRYING.

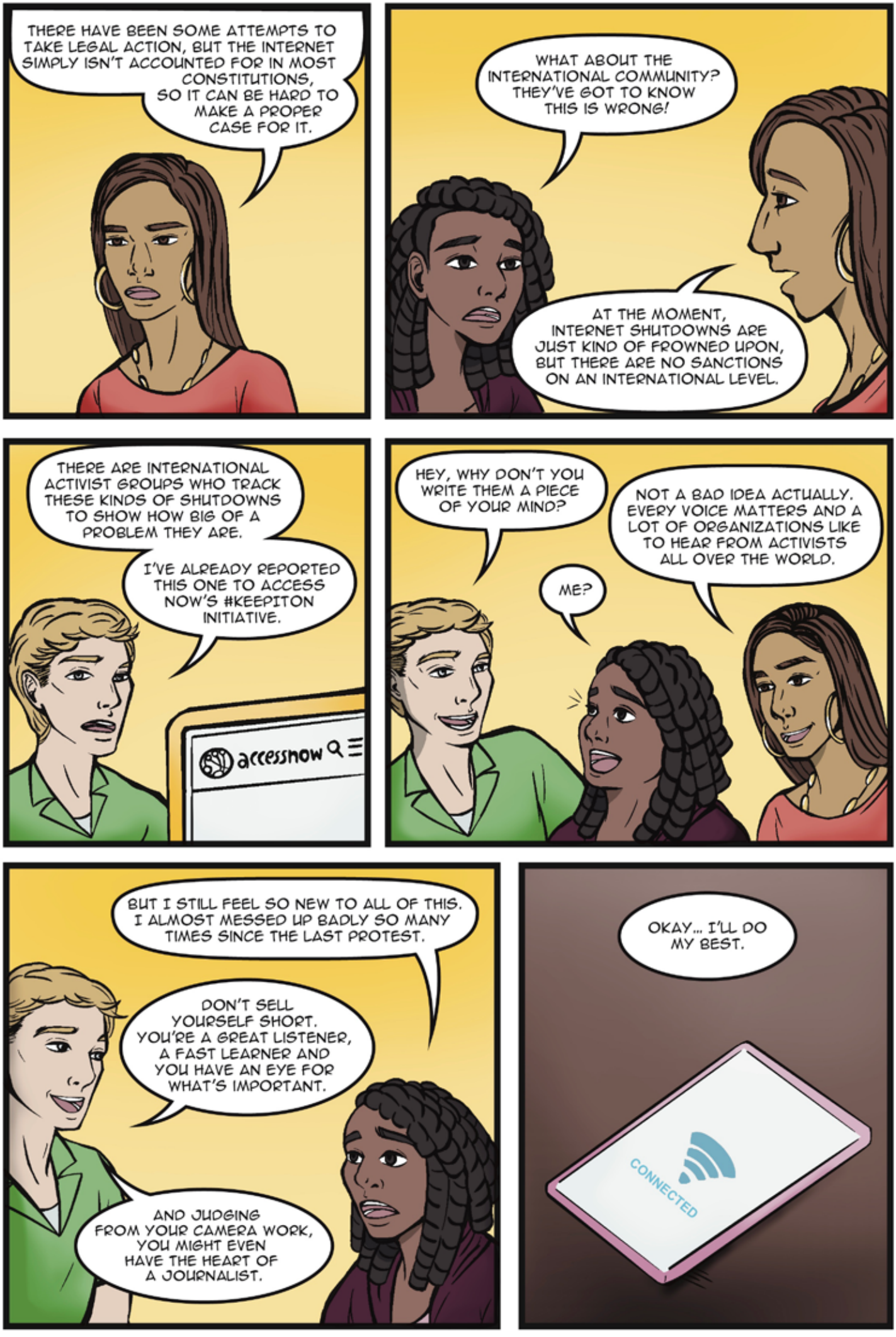

WE'LL BE MEETING WITH A FELLOW ACTIVIST GROUP THIS AFTERNOON TO PROTEST THE SHUTDOWN.
15:30 ON MAIN STREET IN CASE OF A SHUTDOWN WAS WHAT WE SETTLED ON. I MEANT TO TELL YOU EARLIER, BUT THEN THE SHUTDOWN WAS ALREADY HAPPENING.


BUT YOU COULD HAVE STILL CALLED ME OR SENT ME A TEXT MESSAGE, RIGHT? IT'S JUST THE ONLINE MESSENGERS THAT AREN'T WORKING RIGHT NOW.
TOO RISKY. PHONE CALLS AREN'T END-TO END ENCRYPTED LIKE MOST IN-APP CALLS, AFTER ALL.
IF IT'S IMPORTANT AND SAFE COMMUNICATION ISN'T AVAILABLE, IT'S BEST SAID IN PERSON.


WE BETTER BE READY FOR ANYTHING. ONCE THE INTERNET SHUTS DOWN, IT BECOMES MORE DIFFICULT TO PRODUCE EVIDENCE OF HUMAN RIGHTS VIOLATIONS.
RIGHT. YOU WANNA GO OVER BLUETOOTH COMMUNICATION REAL QUICK FOR MARIA?


THAT'S ONE SOLUTION, I GUESS...
THE BEST SOLUTION WOULD BE PREVENTING THESE DARN SHUTDOWNS IN THE FIRST PLACE.
BUT IT'S OFTEN HARD TO DETECT HOW THEY'RE BEING PRODUCED AND THE TELECOM FIRMS INVOLVED FOLD TO PRESSURE FROM THE AUTHORITIES.


BY NOW, YOU SHOULD BOTH HAVE AN APP ON YOUR PHONE THAT CAN USE BLUETOOTH TO PASS ON MESSAGES. BLUETOOTH ONLY HAS LOW REACH, BUT THE INDIVIDUAL PHONES CAN USE EACH OTHER TO SPREAD INFORMATION. THE MORE PEOPLE USE IT, THE FURTHER MESSAGES CAN SPREAD IN THIS DECENTRALIZED MESH NETWORK.
CONNECTED DEVICES
THE MESSAGES YOU GET MAY BE CODED SO THE INTENT ISN'T OBVIOUS TO THE UNINITIATED. IN OUR CASE, WE MIGHT BE "GOING OUT FOR PIZZA" AT A CERTAIN PLACE AND DATE TO ASSEMBLE FOR PROTEST.


THERE HAVE BEEN SOME ATTEMPTS TO TAKE LEGAL ACTION, BUT THE INTERNET SIMPLY ISN'T ACCOUNTED FOR IN MOST CONSTITUTIONS, SO IT CAN BE HARD TO MAKE A PROPER CASE FOR IT.
WHAT ABOUT THE INTERNATIONAL COMMUNITY? THEY'VE GOT TO KNOW THIS IS WRONG!
AT THE MOMENT, INTERNET SHUTDOWNS ARE JUST KIND OF FROWNED UPON, BUT THERE ARE NO SANCTIONS ON AN INTERNATIONAL LEVEL.
THERE ARE INTERNATIONAL ACTIVIST GROUPS WHO TRACK THESE KINDS OF SHUTDOWNS TO SHOW HOW BIG OF A PROBLEM THEY ARE.
I'VE ALREADY REPORTED THIS ONE TO ACCESS NOW'S #KEEPITON INITIATIVE.
accessnow
HEY, WHY DON'T YOU WRITE THEM A PIECE OF YOUR MIND?
NOT A BAD IDEA ACTUALLY. EVERY VOICE MATTERS AND A LOT OF ORGANIZATIONS LIKE TO HEAR FROM ACTIVISTS ALL OVER THE WORLD.
ME?
BUT I STILL FEEL SO NEW TO ALL OF THIS. I ALMOST MESSED UP BADLY SO MANY TIMES SINCE THE LAST PROTEST.
DON'T SELL YOURSELF SHORT. YOU'RE A GREAT LISTENER, A FAST LEARNER AND YOU HAVE AN EYE FOR WHAT'S IMPORTANT.
AND JUDGING FROM YOUR CAMERA WORK, YOU MIGHT EVEN HAVE THE HEART OF A JOURNALIST.
OKAY... I'LL DO MY BEST.
CONNECTED

TO WHOM IT MAY CONCERN.

I'M WRITING IN TO REPORT AND SPARK DISCUSSION ABOUT THE CURRENT INTERNET SHUTDOWN IN MY HOME COUNTRY.

INTERNET SHUTDOWNS DIRECTLY INTERFERE WITH PEOPLE'S ABILITY TO EXERCISE THEIR HUMAN RIGHTS.

THEIR RIGHT TO SPEAK.

THEIR RIGHT TO ORGANIZE PROTEST.

THEIR RIGHT TO EDUCATE THEMSELVES.

EVERY ONE OF THOSE WOULD BE OBJECTIONABLE ON ITS OWN, BUT I BELIEVE THE VIOLATIONS EXERCISED THROUGH INTERNET SHUTDOWNS RUN EVEN DEEPER.

HUMANS HAVE AN INTRINSIC NEED TO COMMUNICATE AND TO BE UNDERSTOOD. INTERACTION IS IN OUR NATURE.

SO MUCH SO THAT BEING CUT OFF FROM ALL HUMAN INTERACTION IS KNOWN TO BE A FORM OF CRUEL AND UNUSUAL PUNISHMENT.

SOME THINK THAT THE INTERNET IS "LESS REAL" THAN FACE-TO-FACE COMMUNICATION. BUT IT WAS BORN OUT OF HUMANITY'S NATURAL DRIVE TO INTERACT. IT IS AN EXTENSION OF OUR UNIVERSAL DESIRE FOR COMMUNICATION.

SO HOW CAN A GOVERMENT SHUTTING IT DOWN WHENEVER IT SUITS THEM BE ANYTHING OTHER THAN AN ATTACK AGAINST HUMAN NATURE ITSELF?

I SAY THAT FOR THOSE REASONS, INTERNET SHUTDOWNS SHOULD NOT ONLY BE CONSIDERED IN RELATION TO THE HUMAN RIGHTS HINDERED, BUT ALSO AS A VIOLATION OF HUMAN NATURE IN ITS OWN RIGHT.

I URGE THE INTERNATIONAL COMMUNITY TO TAKE THIS MATTER SERIOUSLY AND TO EMPLOY SANCTIONS AGAINST GOVERMENTS INTERFERING WITH TELECOMMUNICATION THAT CANNOT BE HELD ACCOUNTABLE OTHERWISE.

SINCERELY,
MARIA

SEND

TAKE-AWAYS

Understand the Local Situation:
- You might want to gather insights into the specific local context.
- Check who might be monitoring your activities and evaluate potential threat actors
- Investigate any legal restrictions on tools like VPNs or encrypted messaging apps
- Understand possible consequences, such as penalties or confiscation during inspections.

Keep Software Updated:
- Consider regularly updating all your software, especially security patches, to reduce the risk of vulnerabilities being exploited.

Separate Accounts and Devices:
- You may want to use separate accounts—and if possible, separate devices—for activism to minimize the risk of cross-exposure with personal activities.

Limit Your Digital Footprint:
- Be mindful of linking your real identity to activist accounts. Consider using pseudonyms and avoid real names/photos, especially in messaging apps where strangers access your profile.
- Think twice before uploading photos, videos, or posts that could inadvertently reveal your location, activities, or connections.
- If you want to send a sensitive photo, consider using the 'view once' feature available on some apps. This ensures the recipient can view the image only once and prevents them from taking a screenshot.
- Check your social media connections and be cautious about who you add or follow.

Regularly Clean Your Devices:
- You might want to remove sensitive messages, files, or other digital evidence periodically.
- Don't forget to review your contacts and remove those that may compromise your safety or theirs.

Implement Basic Security Measures:
- Consider creating unique, strong passwords for each account and using a reputable password manager.
- You might want to enable two-factor authentication (2FA) on all accounts, set app-specific PINs, and use automatic app lock features.
- Think carefully about whether to connect to public Wi-Fi networks.

Secure Communication:
- Consider using end-to-end encrypted messaging platforms (for calling too!) and enabling self-deleting messages to reduce risks if your device is compromised.
- Be aware that certain apps may draw suspicion or be criminalized in your region.

Limit App Permissions and Access:
- You could review app permissions and restrict them to essential functions.
- Avoid unnecessary apps, especially those requesting excessive access to your data.

Establish Secure Backups and Recovery Plans:
- You might want to securely back up critical data using encryption to protect it against device loss or confiscation.
- Have a recovery plan ready in case an account is compromised.

Prepare for Device Inspections:
- Consider having a plan for quickly deleting or hiding sensitive information in case of sudden device checks.
- Look into apps or settings that allow you to encrypt, hide, or remove sensitive data and browsing history swiftly.

Stay Alert to Phishing Attacks:
- Be cautious about links, attachments, and messages from unknown sources.
- It's helpful to regularly update your awareness of phishing tactics and verify the authenticity of senders before clicking links or providing information.

By following these steps, you can take proactive measures to protect your identity, your data and your activism efforts in high-risk environments.

For detailed training and technical support, the following websites are helpful:
Front Line Defender: https://securityinabox.org/en/
Helpline Access Now: https://www.accessnow.org/resources/

SECURITY IS PARAMOUNT
–
ONLINE AND OFFLINE

Maria, Alex, Sarah, and Daniel are four friends deeply committed to human rights activism in a country grappling with increasing authoritarianism. Their efforts to organize and amplify their message on social media are met with relentless challenges: internet shutdowns, hacked accounts, direct threats and constant surveillance—tactics aimed at silencing dissent and instilling fear. Daniel's arrest for his involvement in the protests serves as a stark reminder of the dangers they all face.

Follow Maria as she strives to learn more about digital safety and what it means for activists in four short comic stories.