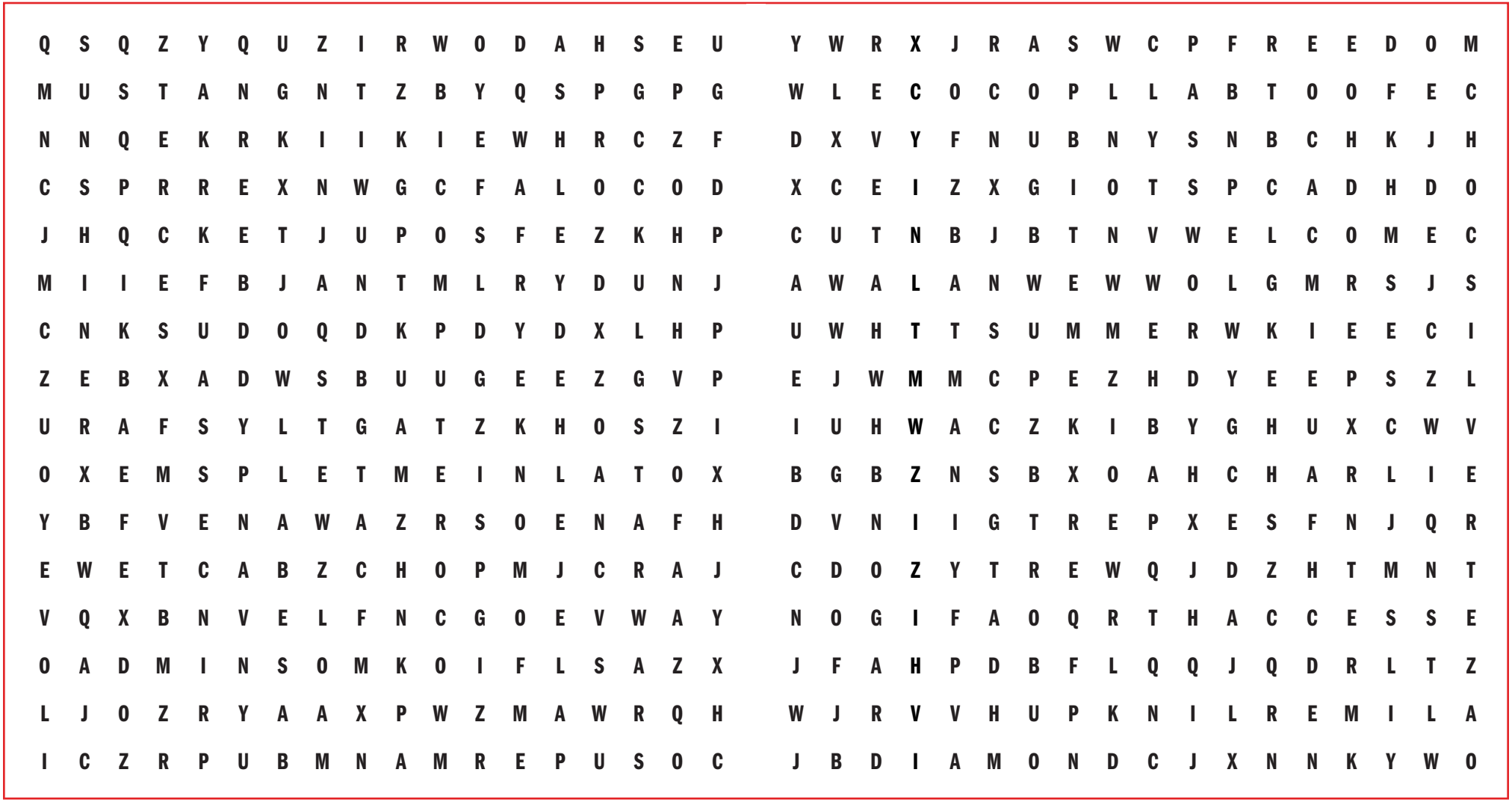
A workbook-style zine to
rethink online security and privacy

(IN)VISIBLE is a response to increasing security and surveillance threats that have emerged with the rise of ubiquitous computing. With these instructional exercises and case studies, you are encouraged to reconsider invisible threats and to envision novel ways of evasion and self-protection.

PASSWORD SEARCH

Two common password mistakes are (1) creating memorable passwords and (2) using the same password more than once. But intuitive passwords that are used on multiple accounts make for easy targets for attackers. To see how simple passwords are easy to breach, find 35 of the most popular passwords in this wordsearch puzzle.

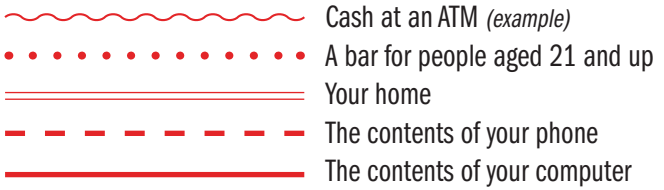
access	biteme	dragon	letmein	monkey	qwerty	summer
ashley	charlie	football	login	mustang	secret	sunshine
admin	cheese	hello	master	ninja	shadow	superman
baseball	computer	iloveyou	merlin	password	silver	welcome
batman	diamond	freedom	michael	princess	starwars	whatever



OPEN SESAME

How do you prove it's you? Multi-factor authentication grants access only after seeing two or more pieces of proof (or "factors"). The 3 common types of proof are knowledge (something you know), possession (something you have), and inherence (something you are). For example, to access cash at an ATM, you use a debit card (something you have) and a numeric passcode (something you know).

Below are common examples of each of these factors. Draw different lines to connect the 2 factors used to access...



KNOWLEDGE	POSSESSION	INHERENCE
Password	Debit card	Fingerprint
Passcode or PIN (Personal Identification Number)	Phone	Voice
Secret question answers	Computer	Face
Name or Username	Photo ID	Retina
Address	Key	

While it might seem like a pain to setup and use two-factor authentication on digital accounts, think about how commonly you're already doing it. You might also consider limiting your use of biometric authentication factors, like your face and fingerprint. They might be convenient to use, but just think – if any of these factors were hacked or stolen, which would be hardest to replace?

DIGITAL FIRE

When you consider how much of your life is online, it can be a bit overwhelming to think about how to protect it all. It may be helpful to start by thinking about what is *most important* for you to keep secure. If all of your digital accounts were suddenly on fire, what would you save?

To understand what you value, rank order the following list of service categories with 1 = most important and 10 = least important:

_____ Banking and finance

_____ Email and messages

_____ File storage (photos, documents, etc.)

_____ Health and medical

_____ Music streaming

_____ Shopping (clothes, books, etc.)

_____ Social media

_____ Travel (airlines, hotels, etc.)

_____ Transportation (ride sharing, food delivery, etc.)

_____ Video streaming

Without thinking too much about it, you've just engaged in "threat modeling," or thinking about what hackers might desire and where you might be vulnerable. Now that you've prioritized what's most important to you, focus on how best to safeguard these accounts like using strong passwords and setting up multi-factor authentication.

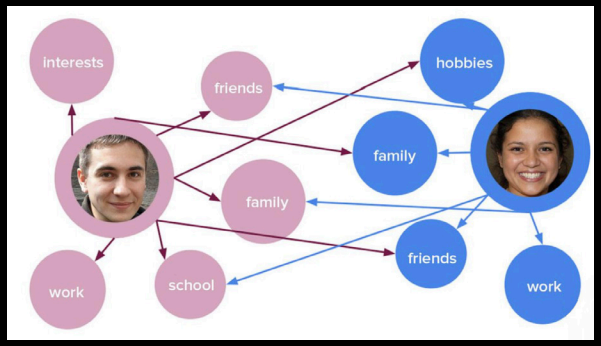
MAKING NOISE

Scholars Finn Brunton and Helen Nissenbaum propose obfuscation, or the deliberate use of ambiguous, confusing, or misleading information, to interfere with surveillance and data collection projects.

NOISZY is a browser plugin that creates meaningless web data, leaving misleading digital footprints around the internet. This activity dilutes the significance of your "real" data, making it more difficult for an algorithm to understand, market to, or manipulate you. Get the plugin at noiszy.com.

GO RANDO is a web browser extension by Benjamin Grosser that helps to evade emotion profiling. Every time you "like" a post, it randomly chooses a Facebook reaction to make sure you're "emotionally balanced." Install it at bengrosser.com/projects/go-rando/install-go-rando/.

At the 2020 ShmooCon hacker conference, teenager **SAMANTHA MOSLEY** described how she and her friends set up a form of "cooperative obfuscation" by logging into each others' Instagram accounts. More info at shmoocon.org/speakers/#kidsdothedarndestthings.



Loyalty shopping programs allow customers to voluntarily share data about what, where, and when they make purchases. But exchanging loyalty membership info prevents being tracked by retailers. **THE ULTIMATE SHOPPER** project is an example of this in action: by sharing stickers of a Safeway club card barcode, a man named Rob offered other customers to shop anonymously while still receiving "member" discounts. Learn more at cockeyed.com/pranks/safeway/ultimate_shopper.html.

LOOKS PHISHY

Phishing often directs people to give away sensitive personal information at a fake website which matches the look and feel of the legitimate site. What's phishy about these examples?

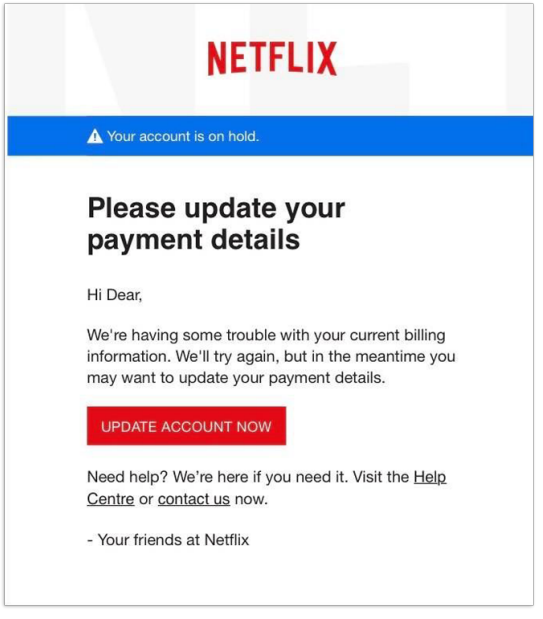
1. _____

2. _____

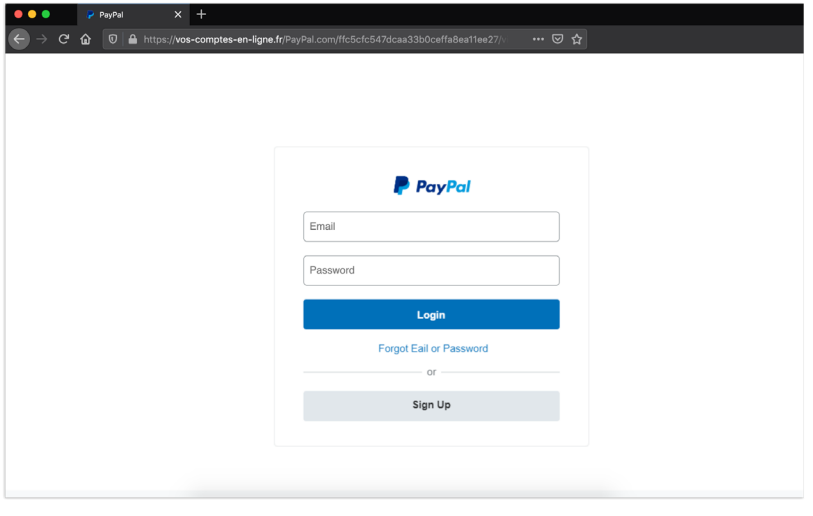
3. _____

4. _____

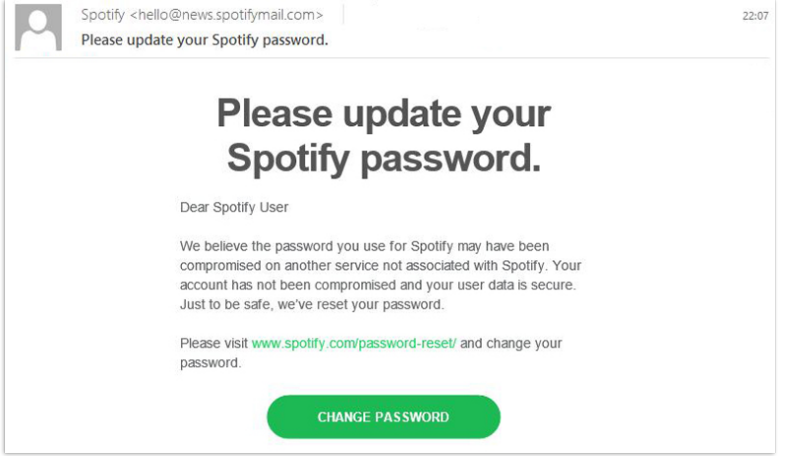
1



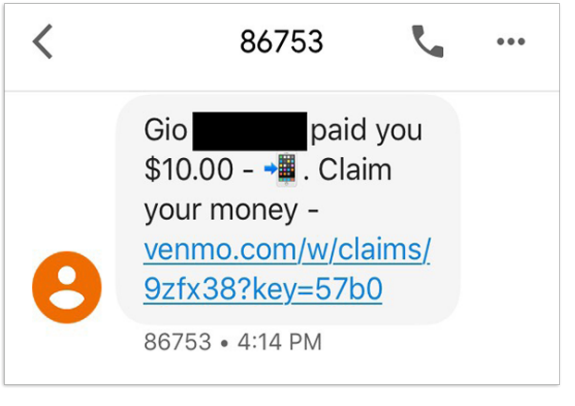
2



3



4



IMAGINING IMPERSONATION

Social engineering involves impersonation to get someone to comply with a request. The attacker often claims to be a trusted authority, and they may gain credibility by stating facts about you and your loved ones that they have previously researched online. After causing you to feel scared or worried about a fake "emergency," they then ask for money or sensitive information to handle it on your behalf.

Imagine you were attempting to impersonate the following people to convince someone to give you $1,000. What would you say?

POLICE OFFICER

INTERNAL REVENUE SERVICE

HOSPITAL REPRESENTATIVE

Now imagine you're on the other end, and you've received these suspicious messages.

What would your first reaction be? How would you verify the person is who they said they were? What are a few different things you might say?

POLICE OFFICER

INTERNAL REVENUE SERVICE

HOSPITAL REPRESENTATIVE

UNDER LOCK & KEY

Why is the lock icon is so commonly used to indicate digital security? Part of it is surely due to its simple, easily recognizable shape. But physical locks and their keys have had symbolic meaning throughout cultural history and around the world.

IRANIAN PADLOCK AMULETS have been ritually worn by pregnant women seeking to prevent miscarriage. Padlocks have also played a part in Persian marriage ceremonies, with the aim to bind the groom to the bride and to symbolize marital fidelity.

During the Qing dynasty, **CHINESE LOCK CHARMS** became popular among parents. The talismans were meant to protect children from death, "locking" them to the earth. Traditionally poorer families sought out support from the community, asking a hundred families for contributions to make a charm for their newborns. Known as a "hundred family lock," these were physical manifestations of a vested interest in the child being secure.

Dating back to late 19th and early 20th century Mali, **BAMANA DOOR LOCKS** provided their owners with more than physical security. With both practical and spiritual functions, locks were believed to be able to keep out evil. Blacksmiths thus rendered both abstract and symbolic door locks: for instance, representing an ancestor on the doorlock offered additional protection by making the door sacrosanct.

KEYS TO THE KINGDOM OF HEAVEN have long signified access to the divine and the authority of the church. Lock and key metaphors in scripture suggest that holiness is the key to salvation. Pictured is St. Peter at a church in Slovenia with the inscription: "I will give you the keys of the kingdom of heaven."

STATUS SYMBOLS

Many of the small icons on top of your phone screen may seem innocuous. But it's important to know what each one means and to pay attention to when it's being used. For example, when your location is being accessed, which app is using it? When you're using wifi, what network are you on – and is it password protected?

To take note of these status symbols, you first need to know them. What do each of these smartphone symbols mean? Match each symbol on the left to the correct description of its meaning on the right. *(Note that compared to Apple iPhones, Android devices have many more possible toolbar icons, and their use can vary widely.)*

APPLE

Your iPhone is connected to the Internet through the Personal Hotspot of another iOS device.

Your iPhone is locked with a passcode or Touch ID.

There's network activity.

Wi-Fi

Your iPhone is connected to the Internet over Wi-Fi.

Do Not Disturb is on. This setting silences calls, alerts, and notifications until you turn it off. Alarms will still sound.

An app or website is using Location Services.

This icon shows the battery level of your iPhone. *(example)*

Orientation Lock is on. Your screen won't rotate until you turn off this setting.

You can use Wi-Fi calling.

ANDROID

Your location is on, and your phone can triangulate your location via GPS, mobile networks, and other features.

Your device is broadcasting to another device.

Your screen orientation (landscape/portrait mode) is locked.

You have a new system update or other important notification.

Your device is uploading data.

Your phone is sharing its data connection as a Wi-Fi hotspot.

You are connected to a password-protected wireless network.

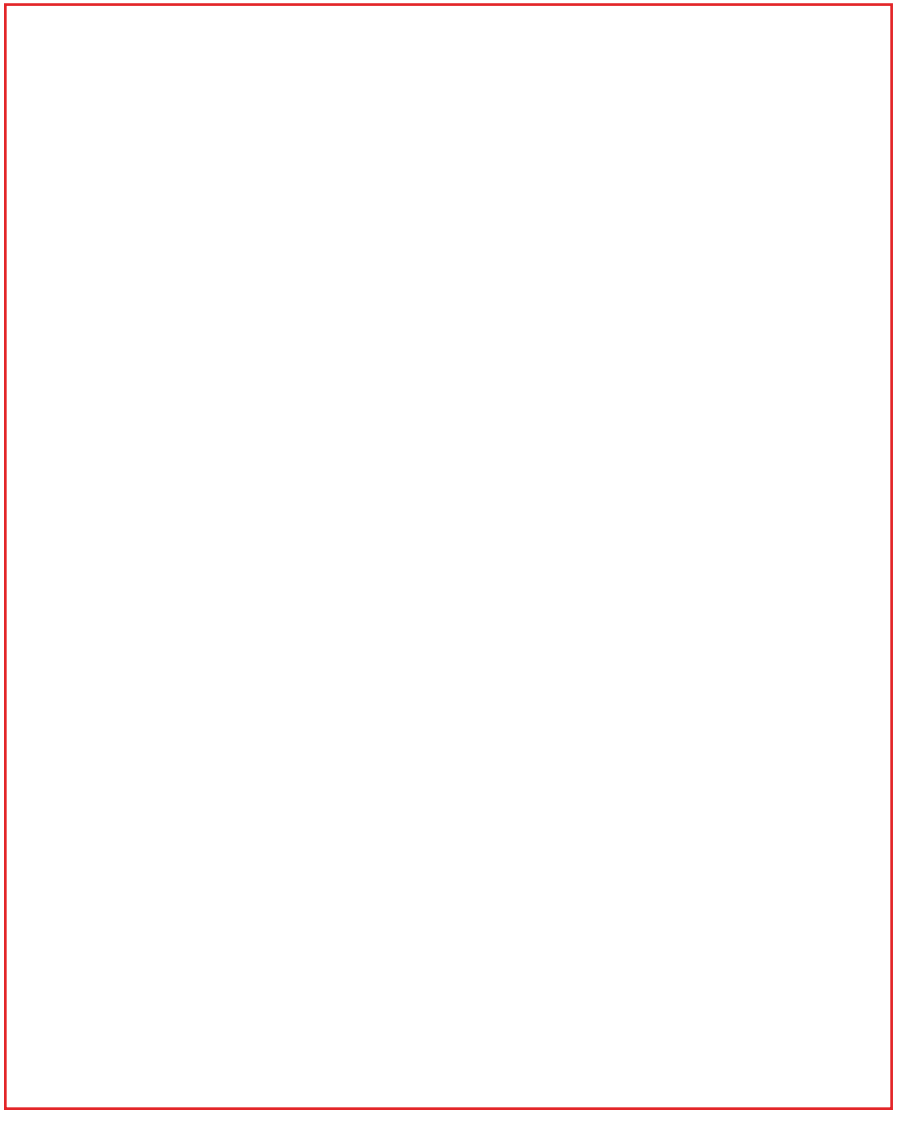
You are using a virtual private network (VPN). Safe Browsing mode is enabled.

Do Not Disturb is on. This setting allows you to customize notification preferences.

A DOODLING INTERLUDE

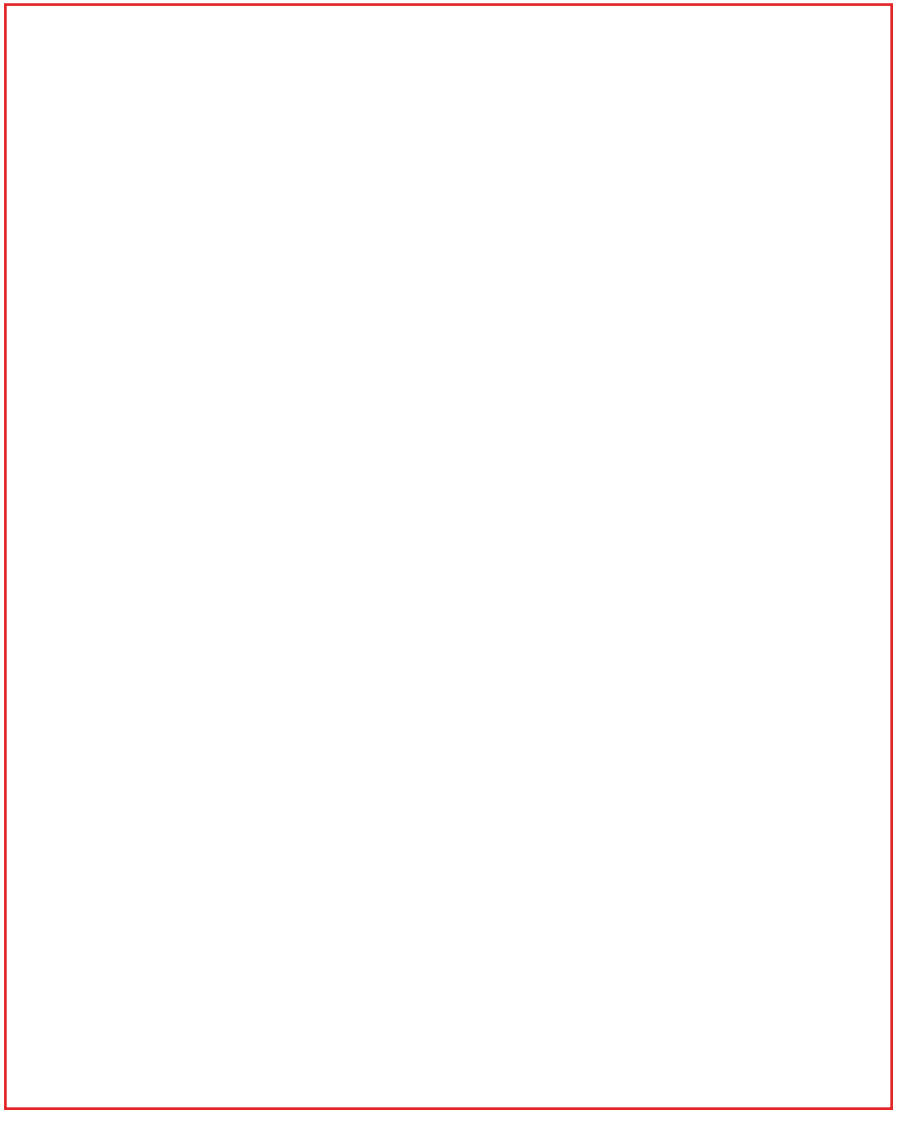
In Maslow's hierarchy of needs, safety and security are basic needs – just above core physiological needs like food and shelter. What makes you feel secure in the physical world? Is it a familiar face, the reputation of a neighborhood, a police officer, etc.?

Draw what makes you feel safe.



Now think about what makes you feel safe online, and why.

Draw what comes to mind. If you can't think of anything, imagine what *would* make you feel more safe online.

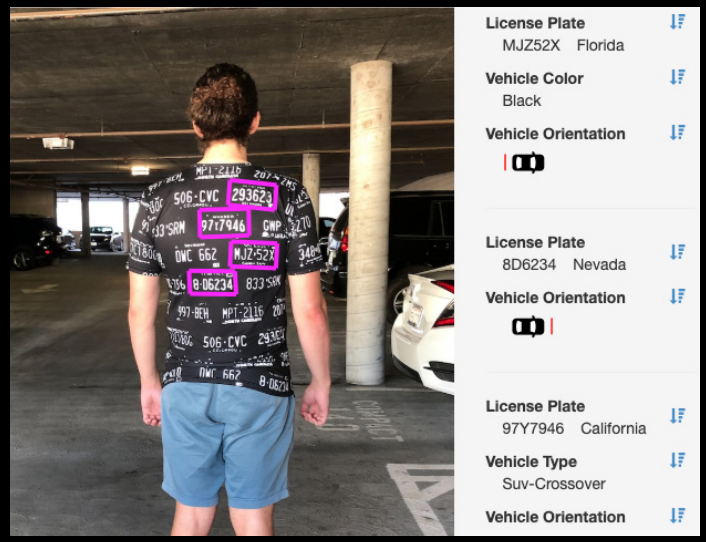


DISGUISES FROM DIGITAL LIFE

A number of artists, activists, and scholars are designing clothing and accessories to enhance privacy in an age of increasing surveillance.

SILENT POCKET makes Faraday sleeves and bags for devices that block everything from GPS and WiFi to Bluetooth and RFID. For sale at silent-pocket.com.

ADVERSARIAL FASHION triggers Automated License Plate Readers, injecting junk data into the systems used by governments to monitor civilians and track their locations. D.I.Y. textile resources available at adversarialfashion.com/pages/diy-resources.

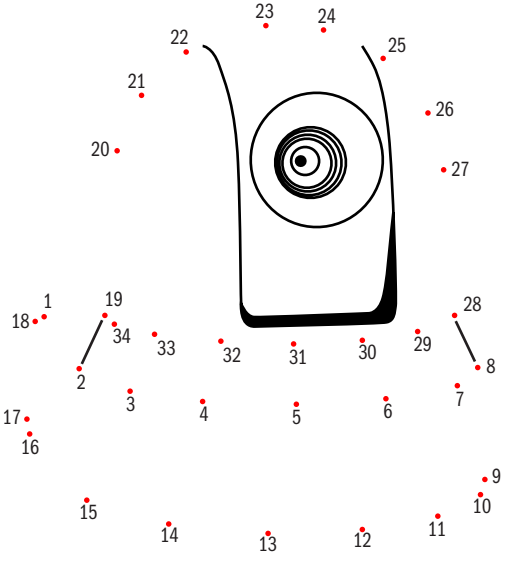


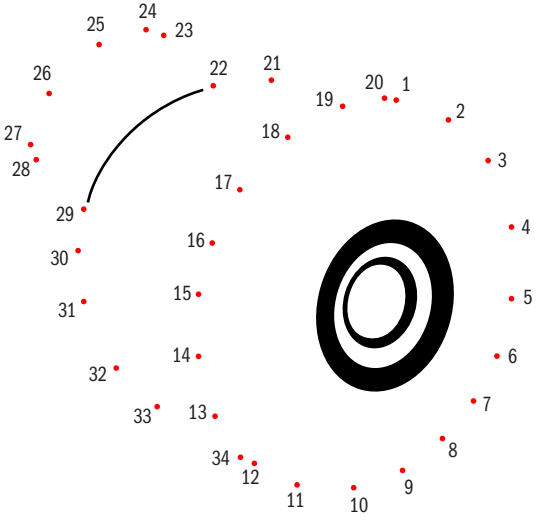
CV DAZZLE is a project by Adam Harvey that uses avant-garde hairstyling and makeup designs to create an “anti-face” and evade facial recognition systems. Style tips available at cvdazzle.com.

REFLECTACLES produces eyewear that block 3D infrared facial mapping during both day & night. They also block 2D video algorithm based facial recognition on cameras using infrared for illumination. For sale at reflectacles.com.

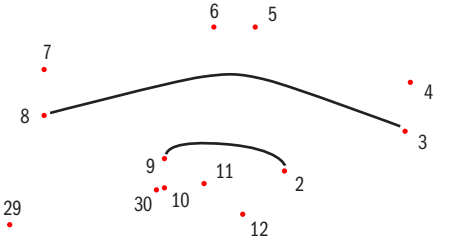
CAMERA SPOTTING

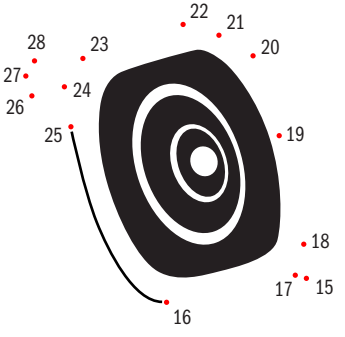
Security cameras are everywhere, from buses and stores to train stations and street corners. Often placed above the eye level, they aren't meant to be noticed. In fact, you may not even recognize a camera if you saw it. To help you start to recognize surveillance cameras, connect the dots to see what a few different types look like.

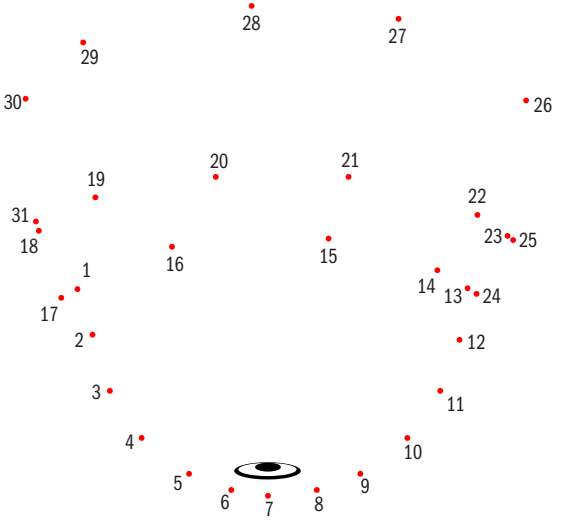




As you start to notice security cameras, how many do you see on a daily basis? Where are they most and least commonly placed? Why do you think that is?





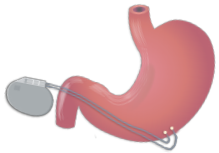


OPERATION BODY GUARD

Someone hacking into an account or device often feels less serious than someone breaking into your house or car. But digital harms from security and privacy breaches can be as severe as physical harms.

As technologies like wireless earbuds and smart watches become mainstream extensions of our bodies, imagine how body modifications, wearables, and medical devices could create new security threats.

Match the potential harms to the different body parts. What other future security risks you can imagine happening to the body?



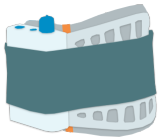
Hacked gastric stimulator leads to nausea and vomiting

Malfunctioning insulin pump leads to seizure

Compromised speaker alters hearing abilities or audio broadcasts and thoughts

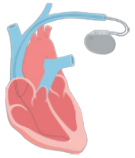
XXX

Breached file storage platform leads to leaked nudes

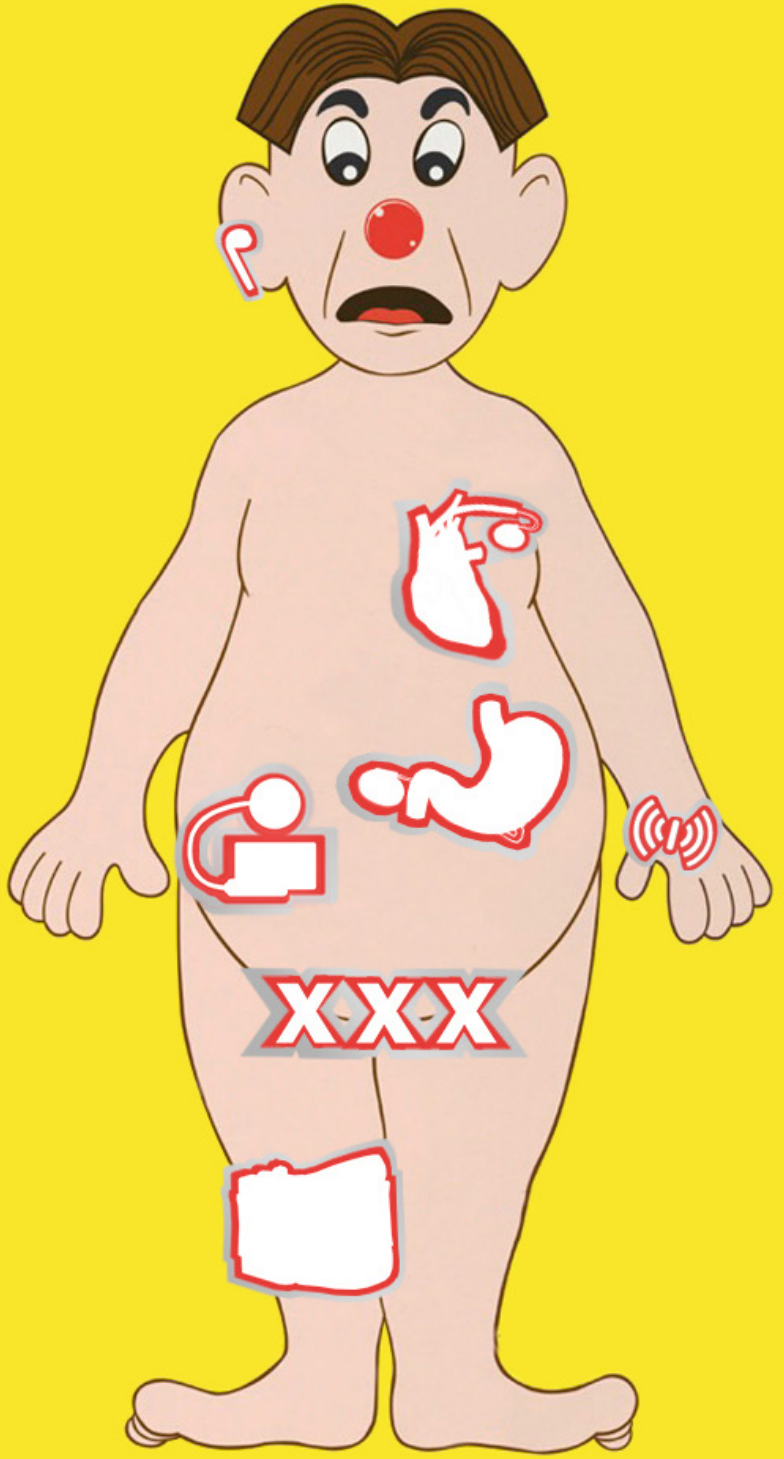


Hacked foot drop wearable device interrupts mobility

Breached NFC implant prevents ability to unlock doors and make payments

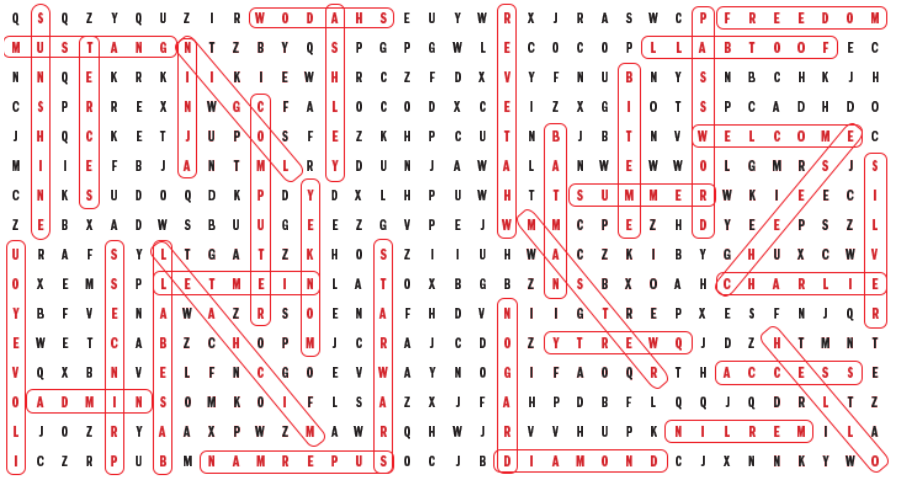


Compromised pacemaker leads to sudden cardiac arrest



SOLUTIONS

WORDSEARCH PUZZLE



OPEN SESAME

- Photo ID & Face
- Address & Key
- Phone & Passcode/PIN or Fingerprint or Face
- Computer & Password or Fingerprint or Face

LOOKS PHISHY

1. Impersonal salutation (“Hi Dear”)

2. Wrong URL, typo (“Eail” instead of “Email”)

3. Suspicious sender (“hello@news.spotifymail.com”)

4. Text message with link (unverified sender), instead of a push notification from the app

STATUS SYMBOLS – APPLE

: Your iPhone is connected to the Internet over Wi-Fi. : An app or website is using Location Services. : Do Not Disturb is on. This setting silences calls, alerts, and notifications until you turn it off. Alarms will still sound. Wi-Fi : You can use Wi-Fi calling. : Your iPhone is locked with a passcode or Touch ID. : Orientation Lock is on. Your screen won’t rotate until you turn off this setting. : There’s network activity. : Your iPhone is connected to the Internet through the Personal Hotspot of another iOS device.

STATUS SYMBOLS – ANDROID

: You have a new system update or other important notification. : Do Not Disturb is on. This setting allows you to customize notification preferences. : Your screen orientation (landscape/portrait mode) is locked. : You are using a virtual private network (VPN). Safe Browsing mode is enabled. : You are connected to a password-protected wireless network. : Your location is on, and your phone can triangulate your location via GPS, mobile networks, and other features. : Your device is broadcasting to another device. : Your device is uploading data. : Your phone is sharing its data connection as a Wi-Fi hotspot.

GOING ANALOG

1. Beware dear reader

2. A foe lies in wait

3. Your message here

SELECTED BIBLIOGRAPHY

Brunton, Finn, and Helen Nissenbaum. *Obfuscation: A User's Guide for Privacy and Protest.* Cambridge, MA: MIT Press, 2015.

"Data Detox Kit." Tactical Tech. Accessed October 18, 2019. https://datadetoxkit.org/en/home.

Grammatas, Angela. "They're listening. Make some noise." Last modified April 22, 2017. https://noiszy.com.

Grosser, Ben. "Go Rando." Last modified August 29, 2017. https://bengrosser.com/projects/go-rando.

Harvey, Adam. "CV Dazzle." Last modified June 15, 2020. https://cvdazzle.com.

Houlbrook, Ceri. *Unlocking the Love-Lock: The History and Heritage of a Contemporary Custom*. Brooklyn, NY: Berghahn Books, 2021.

Mitnick, Kevin, and Robert Vamosi. *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data*. New York, NY: Little, Brown and Company, 2017.

Ng, Alfred. "Teens have figured out how to mess with Instagram's tracking algorithm." *CNet*, February 4, 2020. https://www.cnet.com/news/teens-have-figured-out-how-to-mess-with-instagrams-tracking-algorithm.

Rose, Kate. "DIY Textile Design Resources." Last modified November 27, 2019. https://adversarialfashion.com/pages/diy-resources.

Towne, Schuyler. "Sealed Doors and Crypto Wars." Atlas Obscura lecture series, Online (Zoom), December 2020 - January 2021.

Wu, Amy Sou. *A Cookbook of Invisible Writing*. Eindhoven, Netherlands: Onomatopee Press, 2019.

Created by Joyce S. Lee
joyceslee.com

With support from the UC Berkeley Center for Long-Term Cybersecurity
cltc.berkeley.edu