ONLINE WORKER SAFETY HAZARDS AND CAUTIONS

A PRACTICAL HARM REDUCTION GUIDE ON WHY AND HOW SEX WORKERS CAN PROTECT OURSELVES AT WORK

Version 0.0.1

Hazards research remains ongoing. If you see an issue in your workplace that is not addressed here, go to hackinghustling.com to let us know.

COMMON WORKPLACE HAZARDS

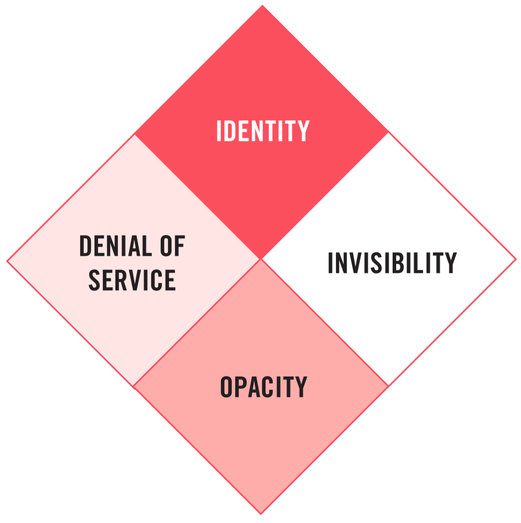
When working for yourself online, there are a few different ways that tools you use for your business can expose you to common workplace hazards. While there are many unique scenarios that produce unique harms, here are a few broad categories of types of workplace hazards you might experience online.

IDENTITY

Doxxing or revealing of alternate personas can happen inadvertently through platform policies and tools, or through a service's complicity with law enforcement. Revealing the contents of your communications can also be a liability if deemed evidence of unlawful activity.

DENIAL OF SERVICE

Working online usually means "using someone else's resources", be they a social media platform or a website hosting service or a credit card processor. These services tend to operate on their own terms, and if they decide your work violates those terms, they can suspend your access to their services.



INVISIBILITY

Is a platform censoring your speech? Are you unable to use your platform? If you can't reach your audience or clients, how will you do your work? (This hazard is often paired with Opacity)

OPACITY

Recommendation algorithms and search engine rankings are opaque to users and companies can change how they work without giving notice to users. If we don't know how a platform works, it usually ends up working against us.

YOUR OWN WEBSITE

LOSING YOUR DOMAIN NAME

If your domain name stops working, first check if it's just expired and you forgot to renew it (usually you'll need to do this once a year, sometimes once every few years). A domain name service can revoke your domain if it violates their terms, but it's not that common.

WHOIS DOXXING

When you purchase a domain name, the contact information you provide is sent to the domain name registrar. An internet tool called WHOIS lets anyone look up the contact information tied to a domain. You can pay for a service to mask your WHOIS records from lookups, and some domain registration services do it by default.

LOSING YOUR HOSTING

If you're using a drag-and-drop website-making service like Wix or Squarespace, these companies can hand your contact information to law enforcement and take down your site if they decide you're violating their terms of service. Sometimes these decisions are automated by image recognition software, sometimes it's not. In any case, it's hard to contest.

SOCIAL MEDIA

BANNING

Social media platforms can decide that your working on their platform is a violation of their terms of service and remove your account. If you have multiple accounts to manage work and personal life, anything that can link those accounts to each other (such as a phone number or mentioning an alt account in a user bio) might be used to ban both accounts. Sometimes your account could be banned if someone–in an act of harassment you might not be aware of–flags your content or account.

SHADOWBANNING

Shadowbanning is something that lots of workers suspect they've experienced, but it is difficult to prove. It means you haven't been removed from the platform, but you're having trouble reaching people–either they don't see you or they can't find you, even though you're active on the platform. Hashtags are censored, users will be unable to see certain accounts in their timeline, accounts will be unsearchable even though the user hasn't been banned. Platforms like Twitter and Instagram insist that shadowbanning isn't actually a thing they do, and generally, at best users can document discrepancies in screenshots and ask others in their network to retweet their content to boost its signal. In some cases, users have found that turning off any auto-posting tools connected to their account or trying to "interact normally"–have more conversational interactions, post non-work related content–can help end the shadowbanning experience sooner.

"REAL NAME" POLICY (FACEBOOK)

Facebook is the main platform that insists that users' accounts display a "real name"–which is something that, for various reasons, you might not want to use professionally. The company is also pretty bad at gauging "real names", sometimes banning users based on their actual but 'weird' name or letting bland fake names persist for a very long time.

PEOPLE YOU MAY KNOW (FACEBOOK)

Facebook's "People You May Know" tool combs through your email address book, your phone contacts, your location history, and your Facebook friends' contacts and location history to try and "connect" you with people on Facebook. It doesn't really distinguish between people having multiple accounts for different personas (work, personal) so your work life might be outed to your friends and family (or your clients might find out your real name and personal connections). It's hard to protect for this because we don't know exactly how PYMK works, but trying to keep these identities separate through how and where you use your digital devices (such separate SIM cards or separate work/life devices, using a VPN for work activities) is a possible mitigating option. If that's not an option, making your alternate account difficult to connect to you on sight (using a real-sounding name unlike your real one, using a profile picture without your actual face) can make it harder for people to connect the personas.

INVITE-ONLY SERVICES

While seemingly private platforms like invite-only forums or startups promising perfect security (which doesn't exist) sound like they would be more secure, they're also extremely interesting to cops who want to infiltrate community.

GIFTS AND PAYMENT PROCESSORS

AMAZON WISHLISTS

Although there are settings on Amazon for hiding your address on your Amazon wishlist, Amazon has recently rolled out a service called "Map Tracking" where products delivered by Amazon's delivery service can be tracked in real time–which means you can see a map of the exact location a product is delivered to. Having a secure address for receiving deliveries or requesting purchases be delivered not through Amazon is not a guaranteed means of protecting your address, but it is an option.

PAYMENT PROCESSORS

Banks are basically the worst, and clients who don't want certain purchases to appear in their bank statements will sometimes flag their purchases to make them go away. This causes lots of headaches for companies like Stripe and PayPal, who lose money when these purchases get flagged. This is one reason why a lot of payment services explicitly refuse to process payments that they believe are "risky." Checking the terms of a payment processor thoroughly is one way to understand your risks before setting up your business services. Additionally, since many online payment processors link user accounts to email addresses, be careful keeping your personal and work contact information separated in your payment services. You may also lose access to your payment processor if someone–in an act of harassment–flags your account for terms of service. Contesting these flaggings can be time-consuming and frustrating.

MESSAGING

EMAIL

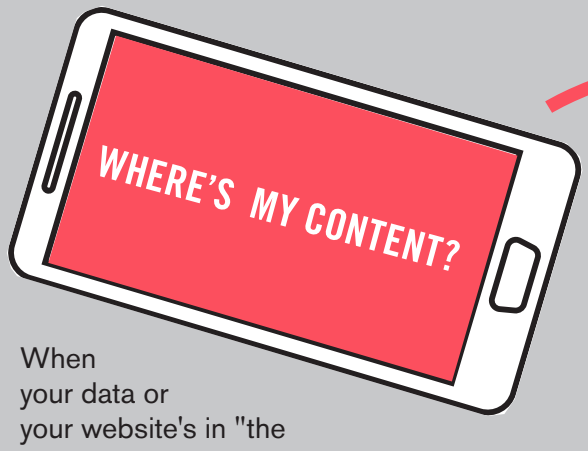
Choosing any email platform will come with trade-offs. Using an encrypted platform might make sense for you, but may not be familiar to your customers. Encryption doesn't protect your communications unless sender and receiver are both using it.

MULTIPLE EMAIL ACCOUNTS

As noted among many other sections in this document, email accounts are often a tool used to connect an online service account to a unique identity. Maintaining clear separation and persona management among these identities can be a challenge.

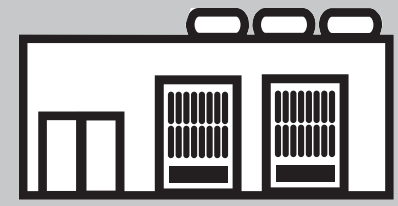
MESSAGING APPS

The number of secure messaging apps (and vulnerabilities and patches to those apps) changes frequently. WhatsApp provides end-to-end encryption, which means both the sender and the recipient's messages are secured. Signal can be used as an end-to-end encrypted option if both sender and recipient are using it, but the app also allows for others to receive messages as unencrypted SMS.



When your data or your website's in "the cloud", that really just means it's on a computer in a data center.

A BUNCH OF COMPUTERS (YOUR WEBSITE OR DATA IS ON ONE OF THEM)



IN A BUILDING FULL OF COMPUTERS

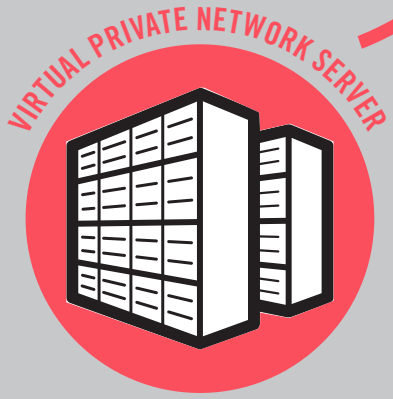
Data centers tend to be concentrated in specific places in the world. It can be hard to know exactly where the computer hosting your content lives unless you have a direct relationship with the hosting provider.

WHAT'S A VPN?

When you're connected to the internet, your online activities can be traced back to the network and the device you're using.

THE REST OF THE INTERNET

When you use a VPN service, your internet connection is routed through another computer somewhere else, so your traffic can be connected to the VPN but not directly to you.



Tor is a little more complicated than a VPN–it bounces your traffic through a bunch of servers, making it harder to trace your online activities back to you.

DOMAIN NAMES

Devices connected to the internet all have an IP address, a unique number ID. Numbers are great for letting computers talk to computers, but try to imagine having to remember something like 170.149.159.130 every time you want to visit a website (try it!). The Domain Name System (DNS) allows people to connect computer IP addresses to human readable (and easier to remember) domain names.

When you're connected to the internet, your online activities can be traced back to the network and the device you're using.

hackinghustling.com

YOUR DOMAIN

- Purchased typically by a third-party service that might also bundle hosting with the domain (like GoDaddy or Squarespace).
- The third-party reseller will send your domain purchase to a domain registrar, who process adding that new domain to a database of domain names assigned to a TLD.
- This means your domain name purchase (and your personal information provided when you buy the domain) can go through a few different hands.

TOP-LEVEL DOMAIN (TLD)

- Owned by domain registries, who maintain records of who has domain names using the TLD (the WHOIS entry)
- There are two types of TLDs: generic TLDs (.com", ".horse") and country-code TLDs, which are all made of two characters and are managed by specific countries (".de", ".is"). Some countries have rules about types of content can be attached to their TLDs and have revoked domains based on content (Libya, .ly. is one past example).

WHAT IF LAW ENFORCEMENT TAKES YOUR DEVICE?

"I Do Not Consent To This Search"
This statement, along with "I am not saying anything without a lawyer", or "do you have a warrant" is probably the only thing you should say to law enforcement. It won't stop a search from taking place, but it is important to have stated on record for future possible legal proceedings.

Does your phone have a passcode?
Number or gesture-based passcodes are a good option here. You can't be compelled to enter your passcode onto your phone for police. However, if you use a fingerprint lock, law enforcement can force your hand onto a device to unlock it.

Are your notifications visible on your lock screen?
A passcode is far more helpful if your lock screen isn't displaying full text of notifications from your messaging apps or your emails. You can change the settings on your device to only provide notification of a message without any of its contents.

Were you separated from your phone at any time?
If police take away your phone or computer and then return it to you, it's possible that the device was tampered with in some way. You probably don't want to keep using that phone.

MORE RESOURCES

HACKINGHUSTLING.COM • SURVIVORSAGAINSTSESTA.ORG • CODINGRIGHTS.ORG/4 • SSD.EFF.ORG • HOLISTIC-SECURITY.TACTICALTECH.ORG

PRODUCED IN COLLABORATION WITH HACKING//HUSTLING:
A PLATFORM FOR SEX WORKERS IN A POST-SESTA WORLD