PRIVACY-MINDEDNESS

Businesses use all sorts of technologies to try to collect information about you, but one of the easiest ways they can collect information is by just asking you. All the technologies in the world won't protect your privacy if you give away sensitive information that you could have kept to yourself.

Here is a list of behaviors that you will want to think about, online and offline, to protect your privacy.

SOCIAL MEDIA

Things you post on social media are analyzed by both the social media company (like Facebook), and third-parties. Some businesses contract with the social media platform to collect your information, while others "screen-scrape," which is basically using automated tools crawl the web and collect what is displayed in websites. In addition, fraudsters can learn information about you from what you share in order to commit identity theft or to con you or your family members. Social media companies encourage you to share as much as possible, but by sharing less (or nothing at all), you are being more privacy-minded.

Similarly, every time you "like," "share," "upvote," or otherwise vote on a post, a band, a television show, a product, or whatever, you are helping marketers and data brokers flesh out a more detailed profile about you.

With the rise of facial recognition technology, whenever you share a photo of yourself you are helping companies do a better job of surveilling you.

Note that dating websites suffer many of the same weaknesses as social media, and people tend to put even more sensitive information there. There are also a lot of scammers there.

Finally, any time someone you do not know contacts you via social media, assume that they are a scammer. If someone you haven't spoken to in a while suddenly wants you to click a link or sends you a video you didn't expect, there's a good chance their account was hacked.

CREATING NEW ACCOUNTS

We have covered the importance of strong passwords and dual-factor authentication.

Many apps and websites let you **log-in using your Facebook, Google, Amazon**, or other credentials. When you do that, you should assume that every transaction you make with that company is being shared with the company you used to log in. These apps usually let you create a stand-alone account by entering your email address and creating a password. It's a little more work but it's a good practice.

Many sites ask you to provide "security questions" in case they need to further verify you. These are actually a terrible practice because it is often easy for a scammer to find out your mother's maiden name or what City you were born in. Consider answering these questions with essentially a password or a nonsense word. It doesn't matter if the answer matches the question – the business isn't checking for accuracy. Just be sure to remember what you answered!

Sometimes a company that you don't really need an account with insists on collecting your email address. If a service requires you to enter an email address, consider using a temporary email address from a site like 10minutemail.com. Similarly, some banks or credit cards will let you generate a temporary, one-use credit card number (a "virtual" number) to enter into shopping sites.

Lastly, some email accounts let you "customize" your email address using the a "+", so if you give your email as "john.doe+1@gmail.com" or "john.doe+BestBuy@gmail.com" then it will work like your regular email, but if you start getting spam sent to that email address, you know who sold your email address!

MESSAGING AND EMAIL

Whenever you send a private message or an email you are taking a number of risks:

1. You are sharing that information with the company that runs the service (and we know that companies like Google and Facebook mine your messages for information);
2. If you are using a school or work-provided service, assume that your employer or school might see the message
3. You are sharing that information with someone who may or may not be trustworthy
    a. or if they're trustworthy now, they may not be trustworthy later after you have had a fight;

    b. or they may accidentally let someone *else* who can't be trusted access their account.
4. You risk accidentally sending a sensitive message to the wrong person (it happens more often than you'd think).
5. You risk accidentally hitting "reply all" when you meant to hit "reply."
6. Even if none of those things happen, email accounts are frequently hacked, either to steal your credentials so scammers can log in as you and access all your messages, or they will just steal all your messages.

Given all of these risks, here are some behaviors you should consider:

- Never send sensitive information like your social security number or credit card number over email or messaging (if a business asks you to do this, it means that business has terrible security practices, so maybe you don't want to use them);
- Never send nude photos or videos over email or messaging (it seems hopeless to try to get people to stop doing this, but the risks of the photos getting out "into the wild" are extremely high).
- Be careful that if you share secrets, off-color humor, or other embarrassing information over email or messaging, an accidental misrouting could have a serious impact on your career or life.
- Remember to never use personal email for business communications.

SOCIAL ENGINEERING

"**Social Engineering**" is the cybersecurity term for when scammers trick you into compromising your security. In other words it's scamming. No matter how tight your security is, all it takes is one person to reveal their credentials to give bad actors their opening.

Online, particular scams you should be worried about include phishing and spoofing – that is emails that seem to be from someone you know and try to get you to click on a link or send money outside. The section on scams covers all of this.

Consider signing up for Vermont's Scam Alerts or stay current with other news sources to be aware of new scams.

In addition, robocallers and phone scammers are so ubiquitous that you might consider simply not answering the phone if you do not recognize the caller. Legitimate businesses generally leave messages. Some phone companies have started providing solutions like AT&T Call Protect and NoMoRobo.

CLOUD SERVICES

Storing things in **the cloud**, whether it's Google Docs, DropBox, Apple's iCloud, or Microsoft OneDrive, carries risks. Some depend on how much you trust the company running the service and how likely it is to get hacked. (Remember when all those celebrities' nude photos got leaked?)

Storing sensitive information locally is always safer. If you are dealing with business information, there might be a policy against storing it on personal cloud storage.

For really sensitive information, consider encrypting the files before storing them in the cloud, either through the native password protection of software like office, or through an application like 7-Zip that can zip and encrypt multiple files.

INCOGNITO MODE

Most browsers have a private or "incognito" mode that provides less information about you to websites and does not store your history. It is not perfect, however, your ISP can probably still see where you are visiting and some websites will still be able to track you. This article provides more information on the strengths and weaknesses of this tool.

BEING A SELECTIVE CONSUMER

Finally, you may have realized by now that some businesses really try to protect your privacy, some businesses don't seem to care about your privacy one way or the other, and some businesses seem to go out of their way to violate your privacy. Be a selective consumer and vote with your dollars (or your eyeballs). Try to support ethical companies, and recommend that your friends and family do as well.

Even if you don't want to be a privacy advocate, you should think about this whenever you are trying to choose between competing products. If you are concerned about privacy, pick the product whose maker has demonstrated a commitment to privacy, and avoid the ones whose makers have not.