


# Opsec 101

by [carrotcypher](#), educational program director at [OSPA](#) 

released under [Attribution-ShareAlike 4.0 International \(CC BY-SA 4.0\)](#)

In this guide we'll cover the basics of Opsec in a way that most anyone should be able to understand. This guide is split up into topics designed to be linked to directly for the purpose of convenient educational discussion. As this is intended for all audiences, it will be rich in easily destroyable strawmen examples that do not necessarily reflect complex realistic threats and risks. If you do not like the included examples, feel free to contribute your own via pull-request.

Note: This guide is not a "how to be anonymous on the internet", "how to protect yourself online", or "best practices" guide. Those are all countermeasure-first approaches that assume a threat model that applies to you (when it often doesn't). Instead, this guide teaches you how to understand that for yourself through the opsec process. While many guides can be useful to learn about potential threats and countermeasures, the countermeasure-first approach of the "[best practices](#)" [fallacy](#) has no place in opsec and ultimately leads to baseless paranoia.

Skip to:

1. [Don't start with countermeasures. Countermeasures come last.](#)
    1. [Thought experiment](#)
    2. ["Best practices" fallacy](#)
  2. [The Opsec process](#)
    1. [What needs protecting?](#)
      1. [Thought experiment](#)
    2. [What is the potential threat?](#)
    3. [What are the potential vulnerabilities?](#)
    4. [What is the potential risk?](#)
    5. [What are the countermeasures?](#)
  3. [Good Opsec? Practice, practice, practice](#)
-



"gate...and no fence!" by apasciuto is licensed with CC BY 2.0.

## **Don't start with countermeasures. Countermeasures come last.**

A countermeasure literally means a measure of response to counter a threat. Countermeasures can be:

- The browser you use to hide your fingerprint on websites
- The lock on your front door to keep home intruders out
- Your VPN that helps hides your location
- Stronger passwords, password managers, key based logins, etc are countermeasures to frustrate attempts to gain unauthorized access

Each of these countermeasures is designed to counter a specific threat. So why not use all of them "just to be safe"? In order to see why that thought process is flawed, let's take the countermeasure-first approach to the extreme.





"After the Fall, People Have Poorly Painted Doors, and Put Lots of Locks on Them" by Rich Pianka is licensed with CC BY-NC-SA 2.0.

### Thought experiment

☐ If adding a deadbolt on your doors makes your home safer overall, why wouldn't you want to add one to every door in the house?

While it might serve to slow down and frustrate a home invader, it would also mean everytime you go to the bathroom, kitchen, or anywhere in your house you'd be pulling out a key and locking/unlocking doors. This level of countermeasure might be necessary for inside a bank, but for most peoples homes it would only complicate life and potentially increase liability if there is an emergency.

☐ If VPNs hide your location, why wouldn't you want to always use one all of the time?

VPNs might work to hide your real IP address from questionable websites, but websites such as government or banking websites use that data to confirm your real identity. Spoofing that can cause complications such as account freezes.

☐ If using strong passwords and changing them often makes you safer, why wouldn't you want to change your phone's

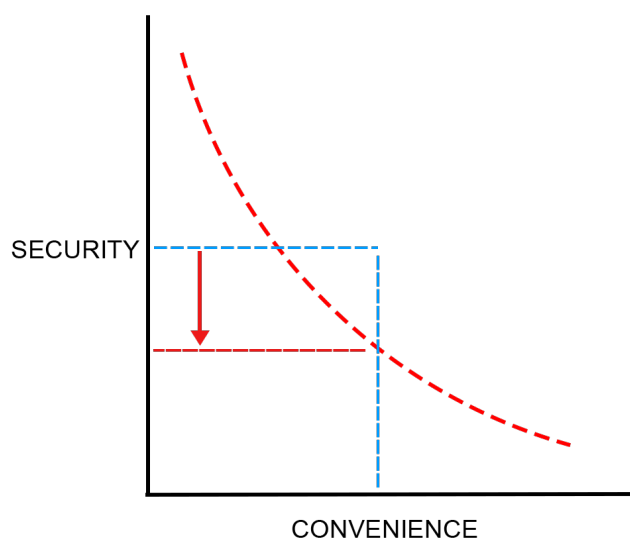
password everyday to a new 1024 character length passwords made up of random characters?

Depending on how often you need to use your phone, having a long password to unlock it may make you unproductive at best. Imagining entering a password that takes 10 minutes to type out every time you want to respond to a message. This might make sense for a device that gains access to a government's nuclear control facilities, but for most of us it is far beyond the point of diminishing returns.

It's quickly evident that without a rational threat or otherwise clear reason for a countermeasure, you end up spending time, energy, and even money for little to no benefit on a threat that may never materialize. Worse, in doing so you can increase your liability and attack surface.

The countermeasure-first approach is unsustainable, misleading, and fundamentally ignores two critical paradigms:

5. Convenience is inversely proportional to safety and security. The more secure we make things, the less convenient they become and the more liability or vulnerabilities may be introduced.



6. The more you attempt to secure something, the more attention it can bring, potentially increasing threats. Often, hiding in plain sight is more effective.

To combat this, we put countermeasures in the back and focus on the rationale first. This is called the opsec process. The opsec process is a list of questions to help rationally assess a threat and judge the efficacy or even necessity of countermeasures against it.

[!\[\]\(c50c8b7b2cc2cf9ff925edec0ee94c0d\_img.jpg\)](#) **Food for thought:** Some guides recommend taking a "best practices" approach to security, such as recommending everyone use a VPN, password managers, etc. This "best practices" fallacy is a countermeasure-first approach based on the study of successes, rather than failures, and as such is an insufficient starting point when assessing any highly-individual and dynamic topic such as security or privacy.

In reality, while the countermeasures recommended might end up working for some of the people, some of the time, that merely indicates the threat model for those people happens to be similar at the moment, but it doesn't teach why, nor is it adaptable for when it's not similar. This is why rather than making assumptions based on the "best practices" fallacy, Opsec seeks to understand the rationale to make reproducible judgments in dynamic situations, to educate oneself through practice to the point of not needing any guides.

[top](#)

---

## The Opsec process

Opsec is a practice or methodology based on rational assessments before action. Before deciding what countermeasure to use, first you need to assess if the threat is serious, or even practical.

This is done by asking a series of questions in order.

---

## 1. What needs protecting?

This could be information, a physical item, your personal health, or anything that has value or provides additional opportunity once accessed. For most of us, the answer to this question might be family, our home, any number of valuable belongings, our personally identifiable information, important financial information, or our passwords. All of these things need to be protected, but not all of them are always at risk in every situation.

### Thought experiment

☐ Have you ever left your phone on a desk at work while turning your back on it to talk to a colleague? Couldn't it have been stolen in that moment?

Depending on what your relationship is with your colleagues, the level of safety common in said workplace, the type of workplace, and the value of the phone, information on it, or access it provides, that phone may either need to be handcuffed to you or can be lent to a colleague unlocked without incurring any risk at all.

☐ Have you ever left your front door open while carrying multiple loads of groceries or moving boxes from the car to the living room? Couldn't someone have entered into the house in that moment?

The physical safety of keeping our doors open is based on the likelihood of someone trying to enter. You can usually visually inspect your surroundings well enough to see if that is a likelihood or not, but how serious to take this will likely depend on the safety of the neighborhood. Some neighborhoods you could leave your door open all day long without incurring any risk. Others, adding a security door to your house may just get it stolen in the night.

☐ Have you ever given your credit card to a cashier and trusted them to charge it only for the amount of the goods being purchased? Couldn't they have charged a much larger amount or even stolen your card number for later personal use?

While theft and fraud do happen, usually the bank and law enforcement resolve these issues for you. The likelihood of these things happening to you largely depend on the type of establishment and the risk/reward ratio for the individual. The risk of getting fired or going to jail deters most undetermined criminals.

The fact is, whether something needs protecting in that moment or not largely depends on what the threat might be, or more importantly the practicality of a threat at all. Just as it's highly unlikely a worker in your office would steal your phone from your desk, it's also unlikely your stolen phone would garner much value to them if properly locked and devoid of any real useful information on it (*an example of an applied countermeasure*).

[top](#)

---

## 2. What is the potential threat?

Most people don't need help identifying common, obvious, physical threats. We encounter enough of those in the course of our daily lives that it becomes a second nature for most. While identifying them, we tend to internally ask ourselves questions to assess the potential threats.

- What time is it? 2am? Why is someone at my front door? What would they want? What are they wearing? Do they look suspicious otherwise?
- Who is that in the alley with me? Do I know them? Are they far enough away that I am safe? Are they following me or just walking the same direction?
- Why is that person at the ATM so close to me? Is it accidental or on purpose? Are they elderly or blind perhaps?

But not all potential threats are so obvious to everyone, especially abstract ones related to the effects of running certain software, performing certain actions on a computer, or trusting certain sources of information.

☐ You sign up for a website to buy your friend a gift and there's only one left! Out of convenience you use the same username and password you do for another site. What could go wrong?

The website you provided information to has its database hacked and subsequently leaked on message boards of hackers who will now try those same credentials at various sites in hopes of gaining access to your life and finances.

☐ You're on a flight and need to use the paid wifi with your credit card. What could go wrong?

While entering your credit card, the passenger in the seat behind you takes a photo of your card and uses it to order the wifi also.

☐ You see someone fall over in the street in front of your car and you get out to help them. What could go wrong?

They start screaming that you hit them with your car (when you clearly didn't) and call the police and demand compensation. Alternatively, while you're helping them, someone hops into your car and steals it.

These threats are all possible, but perhaps unlikely. Still, it's important to try to brainstorm and identify potential threats as early as possible: before you leave on that vacation, before you start your car, before you enter your information into that website's form. Without practicing opsec in this manner, the above threats will need to be learned from experience instead, sometimes at a potentially heavy price.

[top](#)

---

### 3. What are the potential vulnerabilities?

Now that you know what you want to protect (e.g. your credit card on a plane) and what the potential threat is (e.g. the person behind you able to see the card's details or being stolen by other means during the flight), it can be quite straightforward to assess the vulnerabilities and whether they are credible or not.

- Is this the best or most secure way to pay for this service?
- Can someone see my card the way I'm holding it?
- If I were in a different seat, what would I see?
- Is this wifi payment portal really operated by the airline?
- Is the website I'm entering this card information on using a secure (HTTPS) connection?
- Does it share the information with any other services?

Depending on the answers to these questions, you may find that you have none, few, or many potential vulnerabilities. Normally this kind of judgement is possible to do quite quickly, but the more technical the potential vulnerability is, the more experience and knowledge is required. How could someone who isn't aware of HTTPS know that not using it could leak their credit card number to a hacker?

In this particular situation, we eliminate all unlikely or impractical vulnerabilities and focus on what remains.

- Someone can see you typing the credit card information on your phone.
- Someone can see your physical card.

[top](#)

---

#### 4. What is the potential risk?

It's important to know the difference between a vulnerability and a risk. Simply put, the vulnerability is **how** it might be possible to attack you. The risk is **what you could lose** if it succeeds.

Now that you know the potential threat and potential vulnerabilities, you can ask the more practical questions about the realistic potential risk to you. This is where common sense, rationality, and statistics will serve you well. **There is no room for fear and paranoia in this step.**

- How much money is on this card?
- How much could be lost?
- How much can I afford to lose if I make a mistake?
- How difficult, time consuming, and inconvenient will it be if I need to order a replacement card if it's stolen?
- Are there any passengers near me that could steal the information in the first place?
- Is the risk worth the trouble for some wifi?

Assuming a credible risk is perceived, the next step is to assess which countermeasures are most appropriate for the threat.

[top](#)

---

#### 5. What are the countermeasures?

Assuming a credible threat exists and there is perceived risk, the next thing to do is to apply the countermeasures to close up the vulnerabilities that will ultimately serve to neutralize the threat.

In this particular situation, we have eliminated all unlikely or impractical vulnerabilities and focus on what remains.

- Someone can you typing the credit card information on your phone.
- Someone can see your physical card.

The easiest countermeasure for these is likely the same for both:

- Cover your phone and card with a coat, or hold it down in your lap away from the line of sight of any other passengers until the process is complete.

The simplicity of assessing a specific threat and risk may lead one to believe the thought process isn't being used, but much like math, just because an easier equation doesn't need a calculator doesn't mean there isn't calculation occurring. The simplicity of the process can be deceiving and lead to the belief that applying a countermeasure-first approach is sufficient. That is the ["best practices" fallacy](#) addressed earlier.

[top](#)

---

## Good Opsec? Practice, practice, practice.

The previous examples were largely obvious and wouldn't necessarily need a guide or checklist to assess them. What's important is the thought process behind them: to be asking the right questions and learn how to find the right answers in a reproducible way.

In the following section, we'll take the opsec process to less simplistic scenarios, gradually increasing the difficulty of these scenarios in story form to uncover gaps in knowledge and get better at applying the opsec process instinctively.

**Work in progress:** This document is a work in progress. Expect occasional updates that change the content, design, and length of the document.



This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).

See an issue with this page, want to add your own information, or feel like providing a translation? [Visit this page on github](#).