bitwarden

The hacker’s guide to securing your organization

Strategies to safeguard your company’s assets and reputation from hackers like me!

Rachel Tobac

Technology moves fast. And so do hackers. But, you know what doesn't move fast? Human habits. Our brains are wired to fall for the same scams we've been falling for since the dawn of time. Even now, people and companies get hacked in the same ways - over, and over, and over. But it doesn't have to be that way!

My name is Rachel Tobac and I'm a hacker, an ethical hacker, to be clear. This means companies hire me to tell them where their vulnerabilities are, so I can keep them and their customers safe. As an ethical hacker who's breached the systems of news reporters, billionaires, and everyone in between, I know first-hand how often people fall for very simple principles of persuasion that have stood the test of time, and the technical tools that could have protected them from that fate.

The way to protect yourself and your corporation is three-pronged.

- First, familiarize yourself and your team with the principles of persuasion we use while hacking so you can recognize and shut down the social engineers.
- Next, arm yourself and your organization with the right technology - password managers (or passkey managers), and the right multi-factor authentication for your threat model.
- Finally, because this technology is moving so fast, you can future-proof your security by understanding the risks that are coming next, and the tools you can use to defend against these new threats.

This eBook will give you the knowledge and tools needed to catch even the most cunning of hackers and preserve the integrity of your organization's assets.

Table of contents

The principles of persuasion

The principles of persuasion were extensively researched and popularized by psychologist Robert Cialdini in his book "Influence: The Psychology of Persuasion." These principles provide insights into how individuals can be influenced and persuaded to take specific actions. Hackers often apply these principles when we're hacking organizations through their people.

Applying the principles of persuasion to hacking

Understanding how hackers apply the principles of persuasion is crucial in developing effective defense strategies. By recognizing the tactics hackers and social engineers employ, individuals and organizations can adopt a more "politely paranoid" mindset and implement robust security measures. Building awareness, educating users about common techniques, and promoting a security-first culture are essential steps in combating human-based attacks. Vigilance and skepticism serve as potent shields against the manipulative tactics used by hackers in their quest for unauthorized access.

By recognizing the tactics hackers and social engineers employ, individuals and organizations can **adopt a more "politely paranoid" mindset** and implement robust security measures.

Here are the seven principles of persuasion:

Reciprocity:

When someone tells you information about themself what do you usually do? Reciprocate! It's human nature. Hackers offer something of value to others, whether it's information, assistance, or a favor, and this can increase the likelihood that their targets will be reciprocal to their requests and tell them information about themselves or their organization, for example. If I need to know which operating system (OS) you use to tailor my malware for your machine, I may offer up the OS I "use" to encourage you to reveal the details I need when hacking.

Consistency:

Humans like to be consistent and keep their commitments, especially if we've made them publicly or shared them with others. People are essentially "allergic to being awkward" – if we've given a commitment to someone or made a choice to trust someone, we're more likely than not to stick with that prior choice.

Hackers will try to convince their targets to commit to small actions or statements that align with their ultimate goal, to increase the likelihood of the victim following through on the request. Once a scammer sees commitment, they will often escalate their requests, leading to more significant compromises.

Social Proof:

We tend to look to others for guidance when making decisions. At its heart, this means we're more likely to take certain actions if we see others, especially people like us, doing the same.

> **By posing as reputable individuals or organizations, hackers instill a false sense of trust, making social proof an effective technique for manipulating targets into sharing sensitive information or engaging in risky actions.**

Hackers who manage to convince us that "everybody's doing it" are using social proof to influence our decision-making.

Liking:

People are more inclined to say "yes" to those they like or feel similar to. Hackers will attempt to build rapport, find common ground, and show genuine interest in their targets. Developing positive relationships and appearing to seek genuine connections with others can enhance a hacker's persuasive abilities.

In his book, Influence, The Psychology of Persuasion, Cialdini illustrates this principle with the idea of the Tupperware Party. "The Tupperware Home Parties Corporation arranges for its customers to buy from and for a friend rather than an unknown salesperson. In this way, the attraction, the warmth, the security, and the obligation of friendship are brought to bear on the sales setting," Cialdini writes.

Authority:

People are more likely to comply with requests from authoritative figures or those perceived to have expertise in a particular domain. Hackers will feign credibility, expertise, or authority in a relevant area to enhance their persuasive impact.

Good social engineers leverage the principle of authority by skillfully crafting phishing emails to mimic communication originating from trusted and authoritative entities. They may try to gain your trust by impersonating your co-workers, your boss, your boss's boss, or technical support. **By assuming an authoritative role, hackers increase the chances of victims complying with their instructions, such as providing login credentials or granting remote access to their systems.**

Scarcity:

The principle of scarcity suggests we value things that are limited in availability. When we perceive something as rare, exclusive, or in high demand, we're more motivated to acquire it. When a hacker highlights the unique features, limited quantities, or time-limited offers associated with their proposition, they can create a sense of urgency and increase the offer's perceived value.

The scarcity principle also applies to time. Who among us hasn't been influenced by the "Act now! This deal won't last long!" email?

Unity:

Unity is the seventh principle that Cialdini added in his later work. It emphasizes the power of shared identities and a sense of belonging. **By emphasizing commonalities and aligning individuals with a shared group identity or cause, hackers increase our motivation to cooperate with them and abide by their requests.** When I'm hacking executives, for example, I tend to pretend to belong to the same gym, board, community group, etc.

> These principles provide a framework for understanding how persuasion works and can be applied ethically in various contexts. When used unethically, however, they become manipulation that can be difficult to resist, even when your team thinks they know how to protect themselves online.

Manipulating urgency: exploiting time pressure for compliance

We're all busy. At any given time we have 312 browser tabs open, we're communicating on three different apps on our phones, we're in video meetings while we answer email, and our calendars barely leave us time to eat a quick, sad salad at our desks.

Hackers know this.

Social engineers adeptly exploit the psychological concept of urgency to deceive individuals. They push their targets into hasty decision-making, bypassing critical thinking and rational judgment, compelling us to fall for scams.

Common criminal urgency tactics:

- ✓ Time boxing a request to convince you to take action quickly.
- ✓ Creating urgency by manufacturing an imminent threat or time constraints.
- ✓ Manufacturing urgency by posing as a trusted authority figure or organization and claiming immediate action is required to avoid dire consequences.
- ✓ Inducing panic or fear by emphasizing time-sensitive situations, such as imminent account closure, legal consequences, or financial loss.
- ✓ Using time-limited offers or limited availability claims to pressure individuals into making impulsive decisions.
- ✓ Fabricating urgent situations, such as a compromised account or a security breach, to prompt immediate action and divulgence of sensitive information.
- ✓ Exploiting current events or news topics to create a sense of urgency and capitalize on people's desire to stay informed or involved.

> Skilled cyber criminals capitalize on the natural human inclination to prioritize immediate action over careful consideration, exploiting our vulnerability in moments of perceived urgency to gain compliance and facilitate their malicious intentions.

How to protect your organization… and yourself

Create a strong first line of defense

Creating a strong line of defense against hacking is crucial for individuals and organizations alike. Organizations should prioritize a comprehensive cybersecurity strategy that encompasses human-based social engineering prevention measures, detection systems, technical tools, and incident response protocols.

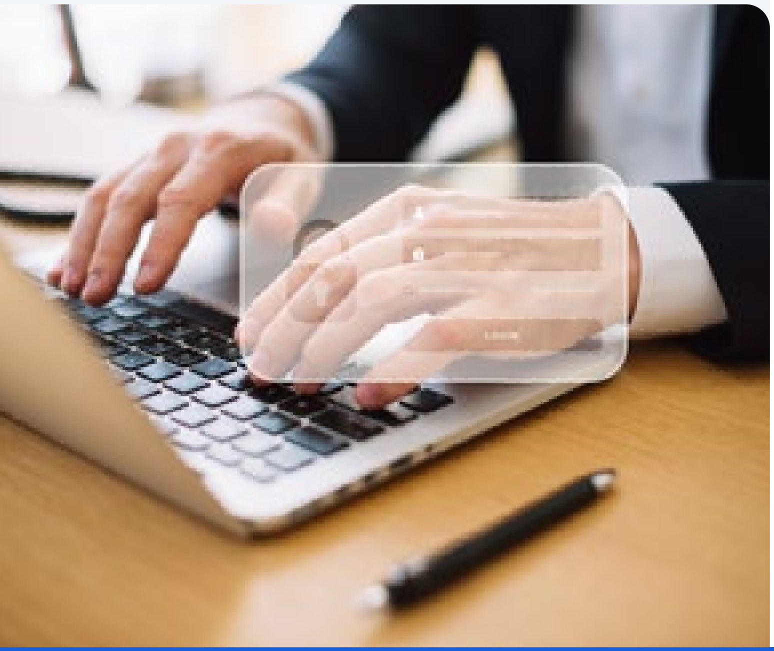
Cultivate a security-first culture in the C-Suite and beyond

Now, getting the security culture right isn't solely the responsibility of the CSO. Everyone in the C-suite plays an important role in emphasizing the importance of a robust line of defense against hackers, reducing the risk of successful breaches, and safeguarding your company's critical assets and reputation.

Importance of unique passwords and password managers

When most people log in to their accounts, they reuse their passwords, or they change the password ever so slightly. And when you reuse or remix passwords and you've been in a breach (which all of us have), that means I can take that password and try putting it into all the other sites you log into – like your bank, work accounts, and personal email.

Bottom line: don't reuse your passwords, it's the very easiest way for me to hack you. If you reuse your passwords across multiple sites, even for sites that you deem silly or kind of a throwaway site. I can take that password and I can use it against you. So you have to use strong and unique passwords for every single site. I recommend storing them in a password manager that keeps all of your passwords safe and encrypted and can generate secure passwords for you.



I cannot overstate the importance of these guidelines in the corporate setting. With the ever-increasing threat landscape, where data breaches and unauthorized access are constant concerns, relying on weak, reused, or remixed passwords is a significant vulnerability. Strong and unique passwords significantly enhance the security posture of an organization.

However, managing numerous complex passwords can be a daunting task. This is where password managers come in. Password managers provide a secure and convenient solution by generating, storing, and auto-filling strong and unique passwords for various accounts. By using a password manager, your team can effortlessly maintain secure, distinct passwords without the burden of memorization (or writing passwords on post-it notes, which I find in the background of pictures on Instagram), significantly reducing the risk of password-related breaches.

In the corporate setting, the adoption of unique passwords and password managers is an integral part of a robust cybersecurity strategy, reinforcing the protection of sensitive data, safeguarding company resources, and fortifying the overall security posture of the organization.

CNN password hacking and password manager video →

Password managers and phishing sites

One of the common tactics employed by hackers is to create fake websites that closely resemble legitimate ones, aiming to trick users into entering their login credentials or other sensitive information. Password managers can recognize phishing sites by automatically matching the login information to the correct website. If a password manager does not recognize the site or fails to autofill the login information, it raises a red flag. This additional layer of verification acts as a safeguard against inadvertently falling for phishing attempts. By relying on password managers, you and your team can have increased confidence in the legitimacy of the websites you visit, making it more difficult for hackers to deceive you with fraudulent login pages or phishing scams.

Multi-factor authentication (MFA) and its significance

Passwords aren't the be-all and end-all when it comes to security. Your teams must use strong and unique passwords stored in a password manager AND multi-factor authentication (MFA).

MFA is a security measure that requires you and the members of your team to provide multiple forms of verification to access a system or account, adding an extra layer of protection beyond traditional username and password combinations. MFA typically combines two or more of the following:

- Something the user knows (such as a password)
- Something the user has (such as a unique code or token)
- Something the user is (such as a finger print or facial recognition

Many people in your organization will recognize and be familiar with MFA since so many consumer apps and websites now offer it, but they might not understand its importance or find the extra step too complicated or a waste of time. Understanding The Why behind MFA is the key to getting buy-in from your team.

The importance of MFA lies in its ability to significantly enhance security by mitigating the risks associated with stolen or weak passwords. Even if an attacker manages to obtain someone's password, they would still need access to the additional authentication factor to gain entry. This significantly reduces the likelihood of unauthorized access and compromises.

MFA helps protect against various security threats, such as phishing attacks and credential stuffing (when hackers find your password in a breach and try to log into your accounts with it). By requiring an additional layer of verification, MFA adds an extra barrier that makes it more challenging for hackers to impersonate legitimate users. It also provides an early warning system, since any unauthorized attempts to access an account will trigger alerts or require additional verification.

Implementing MFA is crucial, especially for sensitive accounts or systems containing confidential information. It helps prevent unauthorized access, data breaches, brand trust loss, and identity theft. By embracing MFA and by convincing everyone else in your organization to use it, you can significantly bolster security and ensure the protection of valuable company assets.

Be politely paranoid: implementing cautious skepticism

Despite our overall busyness and tendency to multitask (even though we know it's not good for focus), we need to be cautiously skeptical in all of our online interactions in order to defend against malicious actors. I call this "Being Politely Paranoid" and it means using two methods of communication to confirm someone is who they say they are before fulfilling their request – a bit like human-based MFA! When in doubt, opt for multi-factor communication. For example, If someone emails you from a new email address requesting sensitive data, call them using the number you already have stored.

A proactive approach to protecting sensitive information can go a long way in maintaining the security of your organization.

By being "politely paranoid" about sensitive requests such as requests for wire transfers, access to company data, bank changes, admin account changes, etc., we can catch cyber attacks in the moment.

How does hacking work?

We know from Verizon's 2023 Data Breach Investigations Report (DBIR) that the majority of breaches are caused by password reuse. Someone may use the same password for their movie streaming site and their email. When the movie streaming site gets hacked, I can plug the exposed email and password from that site into the user's bank and reset all of their other passwords because I have access to their email address.

Most of the time when I'm hacking someone, it doesn't even require that much effort. My first attack method is to determine if I can find the target's password in a breach. Oftentimes, I'm not even targeting a person or organization specifically. Sometimes you and your organization just get caught up in this CSV file with thousands of lines and you happen to be in it because you're a part of the breach – and now your other accounts that reuse that password are compromised in the process.

Open source intelligence

Open-source intelligence or OSINT is a reconnaissance step we take before starting the hack. We try to find as much publicly available information about a target as possible, such as their contact information, technical tools in use, likes/dislikes, etc.

Hackers employ OSINT to query search engines, explore massive public forums, or comb through troves of public records online to find the details needed to launch an attack.

Password dumps

Hackers often find passwords online in what's commonly known as a "password dump." This is simply a massive number of passwords collected from hacked websites, data breaches, or underground forums where cybercriminals trade stolen information. These dumps often contain plaintext or hashed passwords alongside associated usernames or email addresses. Password dumps pose significant risks as they are often the first source of OSINT that attackers leverage to see if they can easily breach an organization's systems. Once a password is found in a password dump, malicious individuals can use it to attempt to gain unauthorized access to user accounts, engage in identity theft, or launch other cyber attacks.

Phishing

Your company can fall victim to phishing scams through various deceptive techniques. Phishing is typically carried out via emails, messages, or fraudulent websites designed to trick employees or individuals within an organization into revealing sensitive information or performing malicious actions.

Attackers may impersonate trusted entities like banks, service providers, or company executives, creating a sense of urgency or importance to manipulate recipients.

(Remember those principles of persuasion?)

Social engineering

Hackers often employ tactics such as social engineering, where they exploit psychological factors to convince targets to click on malicious links, download malicious attachments, or provide login credentials. By mimicking legitimate communication channels, phishing scams can successfully deceive employees into divulging confidential data, compromising network security, or enabling unauthorized access.

Let’s talk threat modeling

Threat modeling is how you determine your level of risk and how likely it is that you’ll experience a hacking attempt. This is how you identify and evaluate the likelihood of receiving potential threats and vulnerabilities in your enterprise. Your individual threat model, for example, is based on many factors such as:

- Are you or your organization in the public eye?
- Are you or your organization currently being targeted in a harassment campaign?
- Do you or your organization support journalists, activists, or other targets of nation state actors?
- Do you speak publicly about your work and role?
- Do you or your organization post in a detailed way on social media?
- Do you or your organization have a lot of followers or attention on social media?
- Do you have to trust a lot of different types of people and roles to get your job done?

The more of these factors you relate to, the higher the likelihood that you will be targeted by cyber criminals more frequently.

The VIP threat model

Imagine me in hacker-mode browsing through social media when I come across a selfie of an executive sitting at his desk working with his dog in his lap. Adorable, yes. But I’m not looking at their goldendoodle. I’m more interested in their laptop in the background. As an exec, they probably know enough not to have their email or any sensitive documents open on their laptop. They’ve minimized all the windows before they snapped the photo and all I see is the beautiful mountainscape desktop scene that they’ve never bothered to change. Now I know what operating system they use and I can instantly tailor malware to work on their machine.

Like I mentioned, folks in the public eye have a high-threat model. This includes anyone in the C-suite of a large corporation. This also includes anyone in your organization with a large following or a person who has access to something that people want, whether that’s money, personal information, or details about a merger and acquisition.

One trick I use in hacking VIPs is called spoofing, which means, I use software to make it look like I'm a VIP on your caller ID but in reality, it's just me on my phone. I'm not actually a board member you need to speak to quickly. I might then invent some scenario to convince you to email me the latest M&A deck to a new email address.

People like your VIPs and executive team have a high-threat model and are more likely than most individuals to receive a targeted phishing attack or to be spoofed over the phone, email, text message or social media. Some execs with high-threat models will experience attempted hacks at least once a quarter, if not once a week. Some people with extremely high-threat models see attempted hacks every single day.

Protecting your VIPs

Protecting individuals in your organization who have high-threat models requires a comprehensive approach that addresses social engineering prevention, physical, and digital security. Here are three key strategies to consider:

Use a second method of communication to Be Politely Paranoid: Make sure that everyone on your team understands common social engineering scams. Encourage all employees to confirm people are who they say they are and build that into your procedures so your team doesn't feel awkward confirming your requests.

Physical Security Measures: Ensure that individuals with high-threat models have access to physical security measures to enhance their safety. Conduct regular risk assessments to identify vulnerabilities in their physical environment and implement appropriate measures to mitigate the risks in their threat model.

Digital Security Measures: High-profile individuals are often targeted or impersonated through digital channels. Implement strong cybersecurity measures to safeguard your VIPs' digital presence. This includes password managers, MFA, encrypting communication channels, regularly updating software and systems, and conducting security awareness training to educate your VIPs about the most common threats they're likely to receive.

Hacking a billionaire video →

How AI has changed the game

Artificial Intelligence has been transforming nearly every aspect of our lives for decades, but since ChatGPT was released, the use of generative AI has exploded. And cyber criminals have taken notice.

Generative AI has revolutionized the landscape of cybercrime, introducing a new era of sophisticated and insidious attacks. Hackers can use AI to impersonate a brand voice or actual voice with uncanny accuracy and precision. This advancement not only raises concerns about the erosion of trust in digital communications but also presents significant challenges in distinguishing between genuine and malicious interactions.

Emulating your brand voice

AI tools have empowered hackers to emulate any brand voice seamlessly. Before these generative AI tools became so accessible, it would take far too long for a hacker to learn to write like a specific enterprise. Only the most artisanal hacker would take the time to study a company's email and website copy.

And if English isn't a hacker's first language, they'd make errors that could make it easier to spot a scam quickly. But now anyone can simply ask a generative AI app like ChatGPT to write in the style of any company and a hacker doesn't even need to speak English well to get the majority of the copy correct. Now hackers have a strong call to action with immaculate copy written in somebody else's brand voice in a language that the attacker doesn't even usually speak.

By using AI to analyze vast amounts of data, these malicious actors can replicate the tone, style, and messaging of well-known brands, effectively deceiving unsuspecting individuals. From spear-phishing emails to fake social media campaigns, AI-powered attacks can be indistinguishable from legitimate communications, leading to devastating consequences for both individuals and organizations. The ability to manipulate brand voices through AI amplifies the already complex battle against online fraud and poses a grave threat to the integrity of digital platforms.

Individuals with high-threat models, such as VIPs, face unparalleled challenges in the AI-powered hacking landscape. As AI evolves, it becomes increasingly difficult to distinguish between authentic and AI-generated content, blurring the lines between truth and deception. VIPs, who are often the targets of sophisticated hacking attempts, must navigate this treacherous environment with heightened caution. They are confronted with the constant threat of AI-generated impersonation, where adversaries can fabricate compelling personas to manipulate and exploit vulnerabilities for nefarious purposes – for example, I was able to impersonate a VIP at 60 Minutes to her team in 5 minutes using an AI Voice Cloning Tool.

60 Minutes video →

How to protect your organization from AI hacking methods

While hacking methods may change, the goals of cyber criminals stay the same. Even if a hacker is using AI methods to impersonate or trick, they are likely still going after the same goals: money, access, data, and influence. Because the goals stay the same during these hacking attempts, many defense recommendations stay the same, too:

- Use strong and unique passwords stored in a password manager to prevent password-based attacks or compromising more accounts after a data breach.
- Use the right MFA for your threat model.
- Use multi-factor communication: Be politely paranoid and use 2 methods of communication to confirm someone is who they say they are before fulfilling their request (you can catch me impersonating an executive's voice during a social engineering call attempt this way almost every time!).

What's next?

Recent data on passwords and password managers

For the third year in a row, Bitwarden partnered with Propeller Insights to conduct a global survey of internet users to understand the state of password management.

The survey probes password habits (including a continued trend of password reuse), cybersecurity risks, and the promise and particularities of passwordless authentication.

Unfortunately, some of the high-level findings show that a lot of folks still have some risky password habits.

- ✓ 19% admitted to having used "password" as their password.
- ✓ 52% have used well-known names, lyrics, or personal names (such as their child or pet).
- ✓ 84% of respondents reuse passwords.
- ✓ 11% reuse passwords on more than 15 sites.
- ✓ 60% have used the same password for 3+ years.
- ✓ 26% of those who reuse passwords have been reusing the same password for more than a decade.
- ✓ 34% still write their passwords down on paper like Post-it notes or a notepad.

Passkeys and the passwordless revolution

Habits are hard to break. Enter passkeys, the vanguard of the passwordless revolution, designed to remove the need for passwords.

Passkeys offer a simpler and more secure way to authenticate. Instead of relying on traditional passwords, passkeys utilize biometric data or other unique identifiers to grant access to digital accounts. By eliminating the need to remember complex passwords, passkeys provide a convenient and user-friendly experience, meeting many people where they're at in terms of digital literacy. Passkeys enhance security by reducing the risk of password-related breaches. Passkeys represent a significant shift towards a future where authentication becomes effortless, efficient, and ultimately liberating for users.

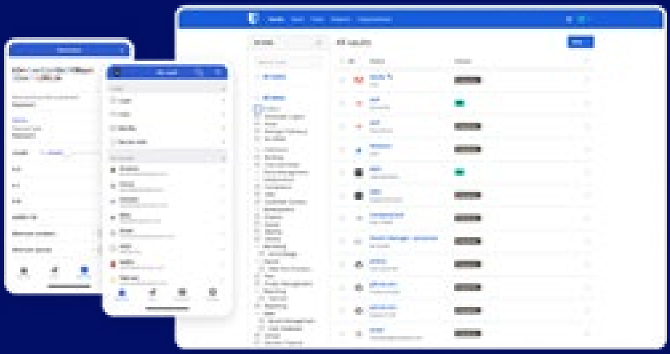
Let me consult my crystal ball

Looking into the future can be scary, but it doesn't have to be. For me, envisioning the security landscape ten years from now sparks an exhilarating mix of optimism and caution. As technology evolves, I foresee a significant decrease in our reliance on traditional passwords. Password-based security measures, prone to human error and vulnerability, will slowly fade into obsolescence. Instead, passkeys will take center stage, transforming the way we authenticate.

However, as we embrace the promise of passkeys, we need to realize this transformation will take time. Security changes slowly – my prediction is that passwords will be around for years to come and we'll gradually transition to passkeys over the next decade.

Bitwarden does both – they've got the password manager for now, and the passkey integrations to support the future of authentication. Now, over to Bitwarden to close us out!

Trusted solutions to keep you and your team safe



Thanks, Rachel – Bitwarden here!

Now that your team is familiar with the threats, it's time to get down to business.

Bitwarden empowers teams and enterprises to effortlessly facilitate secure password sharing among colleagues. It helps reduce cybersecurity risks by implementing robust password policies for all employees and enables monitoring of activities through audit logs. Additionally, Bitwarden seamlessly integrates with your current security tools and supports SSO and directory service integrations. With features like passwordless authentication, biometric unlock, security key support, and credential autofill, Bitwarden ensures that employees can easily access their crucial accounts, thus boosting productivity within your company.

Get started with Bitwarden today →

Contact sales →