

How People Get Hacked Every Day (And Why You Might Be Next)

Assem Hijazi – Experience, Knowledge & Ideas

Contents

- Introduction 3
 - This is a topic people ask about all the time... and it creates real concern. 3
- 1. You Are Already a Target..... 5
- 2. Why Your Data Matters (Why Attackers Care)..... 6
 - What Attackers Want From Your Data 6
 - 1. Money (Direct Benefit) 6
 - 2. Account Access (The Hidden Value) 6
 - 3. Identity Usage (Becoming You) 7
 - The Most Important Idea 7
- 3. How People Actually Get Hacked (Real-Life Methods)..... 8
 - Most Common Ways People Get Hacked..... 8
 - 1. Fake Messages (SMS / WhatsApp) 9
 - 2. Fake Emails (Phishing) 9
 - 3. Fake Calls (Vishing) 9
 - 4. Fake Websites 10
 - 5. Malicious Downloads / Apps 10
 - 6. Password Reuse Attacks 11
 - 7. Social Media Scams 11
 - 8. AI Voice / Deepfake Scams..... 11
 - 9. Public Wi-Fi Risks 12
 - 10. Fake Alerts & Pop-ups (Scareware) 12
 - The Reality You Should Remember..... 12
 - The Key Insight 12
- 4. Why These Attacks Work — Even on Smart People 13
 - Why These Attacks Work (Human Factors) 13
 - 1. Urgency (Act Now) 13
 - 2. Fear (Something Is Wrong) 14

3. Trust (Looks Familiar).....	14
4. Curiosity or Reward	14
5. Distraction (Real Life Moments)	15
The Most Important Insight	15
5. What You Should Take From This (Simple Rules to Stay Safe)	16
Basic Rules to Protect Yourself.....	16
1. Don't Click Immediately.....	16
2. Don't Trust Automatically	16
3. Never Share OTP or Passwords	17
4. Verify from Another Source	17
5. Slow Down	17
6. Use AI as Your Personal Security Assistant	18
How You Can Use AI to Protect Yourself.....	18
1. Check Suspicious Emails	18
2. Verify Links Before Clicking	18
3. Analyze Messages (SMS / WhatsApp).....	19
4. Ask Before You Act.....	19
5. Learn While You Use It	19
Important Note	19
The Key Idea.....	19

Introduction

In this series, I decided to step a little away from AI and focus on something just as important — **your personal security in the digital world**.

However, this time we will also look at AI from a different angle...

👉 Not as a complex topic, but as a **simple tool that can help protect you**.

This is a topic people ask about all the time... and it creates real concern.

Because today, our lives are deeply connected to:

- Phones
- Laptops
- Internet services
- Social media
- And many other digital tools

But while we use these tools every day, most of us are not really sure:

- How safe are we?
 - How do people actually get hacked?
 - And why would someone target us in the first place?
-

The goal of this series is not to turn you into a security expert.

It's the opposite. It's to help **regular users** — not technical people — understand security in a simple, clear, and practical way.

At the same time, we will also use what we already have today — including AI — as a **practical assistant** to help us make safer decisions.

Before we talk about protection, tools, or technical terms... we need to start with something more important: **How attacks really happen in real life**

Because the truth is: Most people don't get hacked because of complex technology... They get hacked because someone convinced them to take one small action.

So in this article, we will start with the basics:

- How people actually get hacked today
- Why your data is valuable
- And what attackers really want

All explained in **simple language**, so anyone can understand — and more importantly, **protect themselves**.

And here is the most important idea to keep in mind from the beginning: You don't need to understand cybersecurity to stay safe... But you do need to understand how people think — including attackers.

And sometimes, you don't need to think alone... You can simply ask the tools available to you — including AI.

This keeps:

- Your original intent ✓
- Adds AI naturally ✓
- Prepares reader for Section 6 ✓
- Keeps it human-centric ✓

1. You Are Already a Target

Most people believe that hacking only happens to:

- Big companies
- Wealthy individuals
- Or people with something “important”

But the reality is very different.

You don’t need to be special to be a target.

You just need to exist in the digital world.

Today, everything around you is connected:

- Your phone number
- Your email
- Your social media accounts
- Your online services

All of these are **entry points**.

And here is something most people don’t realize:

Hackers don’t sit and choose you personally... Most attacks today are **automated and sent to thousands — even millions — of people at the same time.**

You are not being targeted because of who you are. You are being targeted because you are **reachable**.

Think about it this way:

- One message sent to 100,000 people
- If only 1% respond... that’s 1,000 victims

That’s more than enough.

So the real question is not: *“Why would someone target me?”*

The real question is: *“Will I recognize the attack when it reaches me?”*

And this is where everything starts.

2. Why Your Data Matters (Why Attackers Care)

At this point, you might still be thinking: “Okay... *but what do they want from me?*”

The answer is simple: **Your data is valuable.**

What Attackers Want From Your Data

#	Type of Value	What It Means in Simple Terms	Real-Life Example
1	Money	Direct financial gain	Unauthorized payments, bank access
2	Account Access	Control over your accounts	Email, social media, apps
3	Identity Usage	Acting as you	Messaging your contacts, scams
4	Data Selling	Selling your information	Data shared in bulk or dark markets

1. Money (Direct Benefit)

This is the most obvious goal.

Attackers may:

- Access your bank account
- Use your card for online payments
- Transfer money

Even small amounts from many people = big profit

2. Account Access (The Hidden Value)

Sometimes the goal is not money immediately.

It's access.

- Your email
- Your social media
- Your work accounts

Especially important: Your email is like a **master key** Because it can reset passwords for many other services.

3. Identity Usage (Becoming You)

This is where attacks become more dangerous.

Once someone controls your account, they can:

- Send messages to your friends
- Ask for money pretending to be you
- Share malicious links

And people trust it... because it comes from *you*

4. Data Selling (The Invisible Market)

You might think: *“My data is not important.”*

But in reality:

- Data is collected
- Combined with other data
- Sold in large volumes

Even simple information becomes valuable when grouped together.

The Most Important Idea

You don't need to have money to be a target... Your **identity, access, and connections** are already valuable.

That's why attackers don't focus on *who you are*... They focus on **what they can reach through you**.

3. How People Actually Get Hacked (Real-Life Methods)

Now that we understand **why your data matters**, let’s look at the reality:

People don’t get hacked through complex systems... They get hacked through **simple, everyday situations**

Most Common Ways People Get Hacked

#	Method	What Happens in Real Life	Where You See It	Why It Works
1	Fake Messages (SMS / WhatsApp)	You receive a message with a link (delivery, bank, urgent alert)	SMS, WhatsApp	Urgency + curiosity
2	Fake Emails (Phishing)	Email looks like a real company asking you to log in or verify something	Email inbox	Trust in brands
3	Fake Calls (Vishing)	Someone calls pretending to be your bank or support team	Phone calls	Trust in voice
4	Fake Websites	You click a link → website looks real but is fake	Browser	Visual deception
5	Malicious Downloads / Apps	You install something that secretly steals your data	Apps, attachments	Hidden behavior
6	Password Reuse Attacks	Same password used across multiple accounts	Login pages	Weak habits
7	Social Media Scams	Fake profiles, giveaways, or impersonation	Social platforms	Emotional triggers
8	AI Voice / Deepfake Scams	Realistic voice or video pretending to be someone you know	Calls, messages	High realism
9	Public Wi-Fi Risks	Your data is exposed on open or fake networks	Cafes, airports	Convenience over security
10	Fake Alerts & Pop-ups	“Your device is infected” messages pushing you to act	Websites, ads	Fear

1. Fake Messages (SMS / WhatsApp)

You receive a message like:

- “Your package is delayed”
- “Your account is blocked”
- “Click here urgently”

What happens next:

- You click the link
- You land on a fake website
- Or you are asked to enter your details

In seconds, your information is captured.

2. Fake Emails (Phishing)

These emails look almost identical to real ones:

- Same logo
- Same design
- Same tone

They usually say:

- “Verify your account”
- “Your account will be suspended”

What happens next:

- You click the link
 - You enter your email/password
 - The attacker immediately uses them
-

3. Fake Calls (Vishing)

You receive a call from someone claiming:

- “We are calling from your bank”
- “We detected suspicious activity”

They sound:

- Professional
- Calm
- Confident

What happens next:

- They ask for OTP or verification code
 - You share it
 - They access your account instantly
-

4. Fake Websites

You click a link and see a website that looks completely real.

But:

- The URL is slightly different
- The page is controlled by attackers

What happens next:

- You log in
 - Your credentials are captured
 - Your account is accessed
-

5. Malicious Downloads / Apps

This can happen through:

- Email attachments
- Download links
- Unknown apps

What happens next:

- You install the file or app
 - It runs in the background
 - It starts collecting your data (passwords, activity, etc.)
-

6. Password Reuse Attacks

Many people use the same password across multiple accounts.

👉 What happens:

- One website gets hacked
- Your password is leaked
- Attackers try the same password on other platforms

And it often works.

7. Social Media Scams

You may see:

- Fake accounts
- Fake giveaways
- Messages from “friends”

What happens next:

- You trust the message
 - You click or respond
 - You share information or send money
-

8. AI Voice / Deepfake Scams

With modern technology, attackers can:

- Imitate voices
- Create realistic messages

What happens:

- You receive a call or voice note
 - It sounds like someone you know
 - You act based on trust
-

9. Public Wi-Fi Risks

Using open Wi-Fi in places like:

- Cafes
- Airports
- Public areas

What can happen:

- Your data is intercepted
 - Fake networks may capture your activity
-

10. Fake Alerts & Pop-ups (Scareware)

You see messages like:

- “Your device is infected”
- “Click here to fix the issue”

What happens:

- You click the alert
 - You install something or enter data
 - The attack begins
-

The Reality You Should Remember

None of these methods break into systems...They simply wait for you to take one action.

The Key Insight

You are not hacked when someone targets you...

You are hacked when you:

- Click
 - Trust
 - Share
 - Act too quickly
-

4. Why These Attacks Work — Even on Smart People

At this point, you might be thinking: “*I would never fall for this.*”

But the reality is different.

These attacks are not designed for weak users... They are designed for **human behavior**

Why These Attacks Work (Human Factors)

#	Factor	What It Means	What Happens in Real Life
1	Urgency	You are pushed to act quickly	You click or respond without thinking
2	Fear	You believe something is wrong	You try to fix the issue immediately
3	Trust	The source looks familiar or official	You lower your guard
4	Curiosity / Reward	Something interesting or beneficial is offered	You click to know more
5	Distraction / Busy Moments	You are not fully focused	You skip verification steps

1. Urgency (Act Now)

You see messages like:

- “Your account will be blocked”
- “Immediate action required”
- “Last chance to respond”

What happens:

- You feel pressure
- You react quickly
- You don’t verify

And that’s exactly what the attacker wants.

2. Fear (Something Is Wrong)

Examples:

- “Suspicious activity detected”
- “Your device is infected”
- “Your account is compromised”

What happens:

- You panic
 - You focus on fixing the issue
 - You ignore warning signs
-

3. Trust (Looks Familiar)

Attackers use:

- Bank names
- Well-known companies
- Customer support scenarios

What happens:

- You assume it’s real
 - You stop questioning
-

4. Curiosity or Reward

Examples:

- “You received a package”
- “You won something”
- “Important update available”

What happens:

- You want to check
 - You click quickly
-

5. Distraction (Real Life Moments)

This is the most common situation.

You might be:

- Busy
- Working
- Driving
- Tired

What happens:

- You act fast
 - You skip thinking
 - You trust automatically
-

Why Even Smart People Get Hacked

It's not about intelligence.

- Smart people are busy
- Professionals trust systems
- Experienced users move fast

And that's when mistakes happen.

The Most Important Insight

Hacking is not about breaking systems... It's about creating the right moment for you to make a mistake.

Simple Rule to Remember

If something makes you:

- Feel urgent
- Feel afraid
- Feel pressured

Stop. That moment is where most attacks succeed.

5. What You Should Take From This (Simple Rules to Stay Safe)

After everything we've seen, you don't need to remember all attack types...

You just need to follow a few **simple rules**.

Basic Rules to Protect Yourself

#	Rule	What It Means in Simple Terms	What You Should Do
1	Don't Click Immediately	Most attacks need you to click first	Pause before clicking any link
2	Don't Trust Automatically	Messages and calls can be fake	Always question the source
3	Never Share OTP or Passwords	No real company will ask for them	Keep them private, always
4	Verify from Another Source	Don't trust the same message or call	Contact the company directly
5	Slow Down	Most mistakes happen when you rush	Take a moment before acting

1. Don't Click Immediately

Whenever you receive:

- A link
- A message
- An email

Stop for a few seconds.

Most attacks fail if you simply **don't click right away**.

2. Don't Trust Automatically

Even if it looks real:

- Bank message
- Known company
- Someone "official"

Always ask yourself:

“What if this is fake?”

3. Never Share OTP or Passwords

This is one of the most important rules.

No bank, no company, no support team will ask you for:

- OTP
- Password
- Full verification codes

If someone asks → **it's a scam**

4. Verify from Another Source

If you receive something suspicious:

- Don't reply to the same message
- Don't trust the same call

Instead:

- Call the official number
 - Open the official website manually
-

5. Slow Down

Almost every successful attack depends on one thing: You acting too quickly

The Final Message

You don't need advanced tools. You don't need technical knowledge. You just need to pause, think, and verify.

6. Use AI as Your Personal Security Assistant

One of the biggest advantages today is something many people already use... but don't think about for security: **AI assistants like ChatGPT**

You don't need to be a security expert anymore.
You can simply **ask**.

How You Can Use AI to Protect Yourself

#	What You Can Do	How to Use It	Example
1	Check suspicious emails	Copy and paste the email	"Is this email a scam?"
2	Verify links	Paste the link (don't click it)	"Is this website safe?"
3	Analyze messages	Share SMS or WhatsApp text	"Does this look like fraud?"
4	Ask before acting	Describe the situation	"Should I trust this call?"
5	Learn warning signs	Ask for explanation	"What are red flags here?"

1. Check Suspicious Emails

If you receive an email that feels strange:

- 👉 Don't click anything
- 👉 Copy the content and ask:
 - "Is this email real or fake?"
 - "What are the warning signs?"

2. Verify Links Before Clicking

Instead of clicking a link:

- 👉 Copy it and ask:
 - "Is this a safe website?"
 - "Does this link look suspicious?"
-

3. Analyze Messages (SMS / WhatsApp)

If you receive a message like:

- “Your account is blocked”
- “Click here urgently”

Paste it and ask:

- “Is this a scam message?”
-

4. Ask Before You Act

If something feels off — even slightly:

👉 Ask first, act later

- “Someone called me asking for OTP, is this normal?”
-

5. Learn While You Use It

You’re not just protecting yourself... You are training yourself to recognize patterns over time

Important Note

AI is a powerful assistant — but:

- Don’t share sensitive data (passwords, OTPs, full personal details)
 - Use it as a guide, not blind trust
-

The Key Idea

Before you click, reply, or trust... Take 10 seconds and ask.

That small step can prevent most attacks.
