MODULE 2 · FREE COURSE

How Attacks Work



Phishing, malware, ransomware and web attacks, step by step

Start Your Cybersecurity Career

In this module you will learn



The attack lifecycle
How most attacks unfold, from first step to impact



Phishing and social engineering
Why tricking people works so well



Malware and ransomware
The main types and what they do



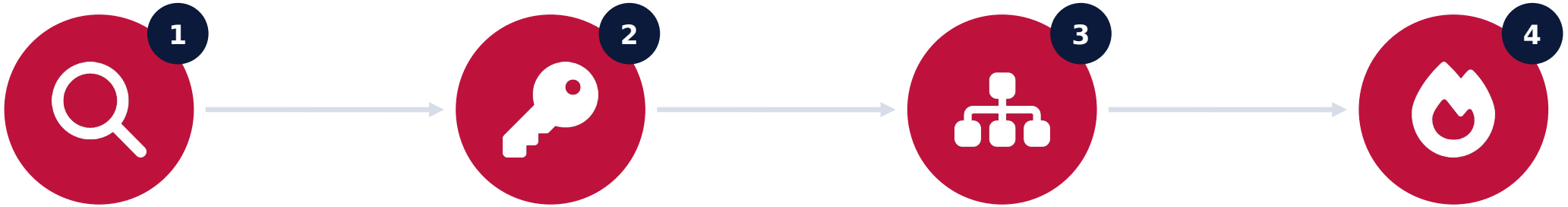
Web attacks
Common weaknesses in websites and apps

02

Module 2 of 8
How Attacks Work

About 20 minutes

The attack lifecycle



Reconnaissance

Learn about the target

Initial access

Phishing, stolen passwords, flaws

Move and escalate

Gain more access inside

Impact

Steal, encrypt or disrupt

Defenders can stop an attack at any stage. The earlier, the cheaper.

Phishing: the red flags

Urgency or fear

“Your account will be closed today.”

Look-alike sender

support@rnicrosoft.com instead of microsoft.com

Suspicious links

Hover first: does the address match the sender?

Unexpected attachments

Invoices or “documents” you did not ask for

Requests for passwords

Real companies never ask for them by email

Money requests

Changed bank details or urgent gift cards

Social engineering beyond email



Vishing

Phone calls pretending to be IT, a bank or the police



Smishing

Text messages with fake delivery or bank links



QR phishing

QR codes that open fake login pages



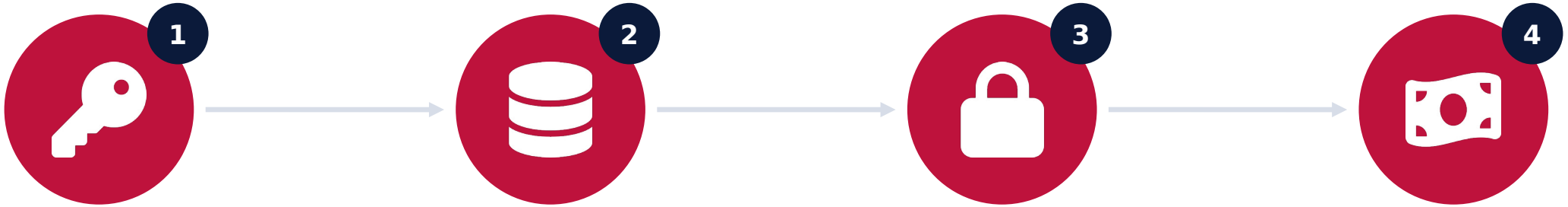
Pretexting

A believable story to get help or information

Main types of malware

Type	What it does	Example impact
Virus	Attaches to files and spreads when they run	Damaged files
Worm	Spreads by itself across networks	Fast, wide infection
Trojan	Hides inside software that looks useful	A backdoor for attackers
Infostealer	Steals passwords, cookies and data	Account takeover
Ransomware	Encrypts files and demands payment	Business stops working

How modern ransomware works



Get in

VPN flaw, stolen password or phishing

Steal data

Copy sensitive files out

Encrypt

Lock systems and backups

Extort

Pay to unlock and to stop the leak

This “double extortion” is why offline backups alone are no longer enough.

Common web attacks

Broken access control

Users can see or change data that is not theirs

Injection

Malicious input runs as commands, e.g. SQL injection

Authentication failures

Weak logins, no MFA, guessable passwords

Misconfiguration

Default settings, open storage, debug pages

Vulnerable components

Outdated libraries or plug-ins with known flaws

Poor logging

Attacks go unnoticed because nothing is recorded

Quick check

1. An email says your account closes in 1 hour unless you log in. Which red flag is this?

2. Which malware type encrypts files and demands payment?

3. In the attack lifecycle, what usually comes right after reconnaissance?

Answers are in the lesson article.

Key takeaways

- Most attacks follow the same stages, and each stage is a chance to stop them.
- Phishing works by exploiting emotions: urgency, fear and trust.
- Modern ransomware steals data before encrypting it.

Next: Module 3 · How Defenders Protect