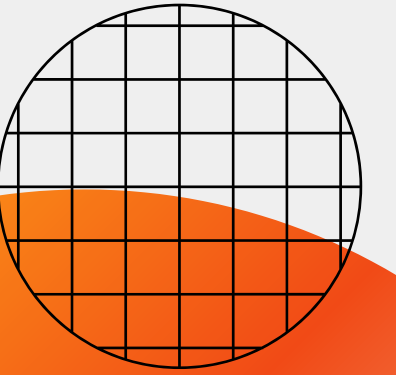


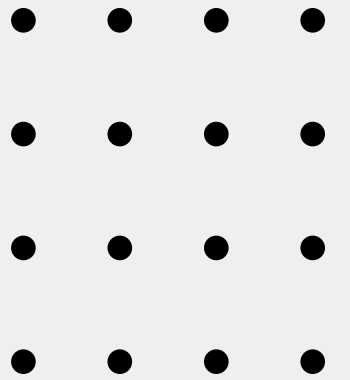
Let's Start

Why Cybersecurity Matters



summary

Objectives
Phishing
Password Security & MFA
Social Engineering
Personal Data Tools
Encryption
Ransomware





Unknown >



Hi there, Daniel — it's Natalia. I'm in a meeting right now and need you to purchase gift cards for a client.

Text me back the codes ASAP, thanks.

Phishing

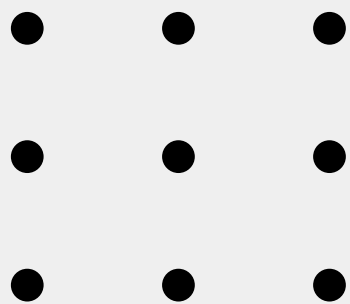
Common types

Email phishing

Spear phishing

Smishing

Vishing



Phishing

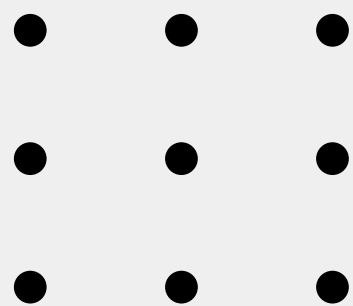
How to Spot Phishing Attempts

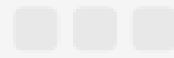
Urgent or threatening language

Suspicious sender email addresses

Requests for sensitive information

Unexpected attachments or links.





https://www.mail.com/yourinbox



Dropbox

<no-reply@dropboxmail.com>

11:00 AM, Today

Hi,

Your Dropbox is full and is no longer syncing files. new files added to your Dropbox folder won't be accessible on your other devices and won't be backed up online.

Upgrade your Dropbox today and get 1 TB (1,000 GB) of space and powerful sharing features.

Upgrade your Dropbox



For other ways to get more space, visit our [Get More Space](#) page.

Happy Dropboxing!

- The Dropbox Team

P.S. If you need the biggest plan we've got, take a look at [Dropbox for Business](#).

<https://www.dropbox.com/buy>

↩ Reply ↩ Reply all → Forward 📁 Archive 🗑 Delete 🚩 Set flag ⋮

Microsoft account unusual sign-in activity



Microsoft account team <account-security-noreply@accountprotection.microsoft.c 

10:36 AM

To: aliveling@live.com

Microsoft account

Verify your account

We detected something unusual about a recent sign-in for the Microsoft account [al*****@live.com](#). For example, you might be signing in from a new location, device, or app.

To help keep you safe, we've blocked access to your inbox, contacts list, and calendar for that sign-in. Please review your recent activity and we'll help you secure your account. To regain access, you'll need to confirm that the recent activity was yours.

[Review recent activity](#)

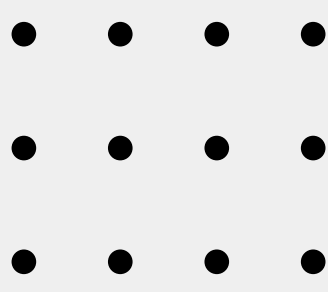
Thanks,

The Microsoft account team



Password Security and Multi-Factor Authentication (MFA)

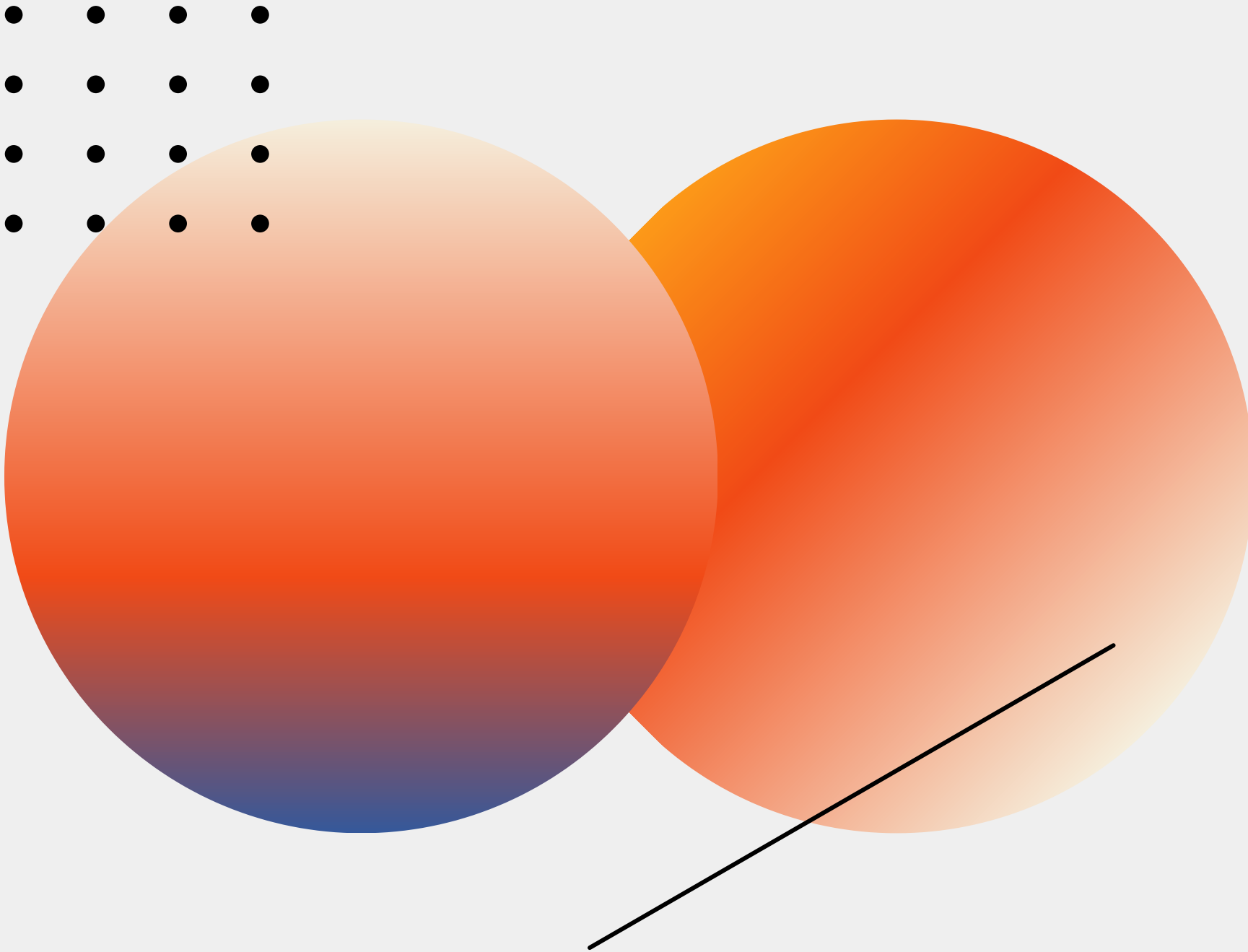
Why Passwords Matter



- Weak passwords are one of the easiest ways for attackers to gain access to accounts.
- Common mistakes:

How to Create Strong Passwords

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
	Instantly	Instantly	-	-
	Instantly	Instantly	Instantly	-
	Instantly	Instantly	Instantly	Instantly
	Instantly	Instantly	Instantly	Instantly
	Instantly	Instantly	Instantly	Instantly
	Instantly	Instantly	1 min	6 min
	Instantly	22 min	1 hrs	8 hrs
	2 min	19 hrs	3 days	3 wks
	1 hrs	1 mths	7 mths	5 yrs
	1 day	5 yrs	41 yrs	400 yrs
	3 wks	300 yrs	2,000 yrs	34,000 yrs



Social Engineering

- 1** Pretexting
- 2** Baiting
- 3** Tailgating
- 4** Quid Pro Quo

Psychological Tactics Used in Cyberattacks

Trust

Attackers impersonate trusted entities to gain victims' confidence.

Curiosity

exploit people's natural curiosity.

Urgency

Creating a false sense of urgency to pressures victims

Authority

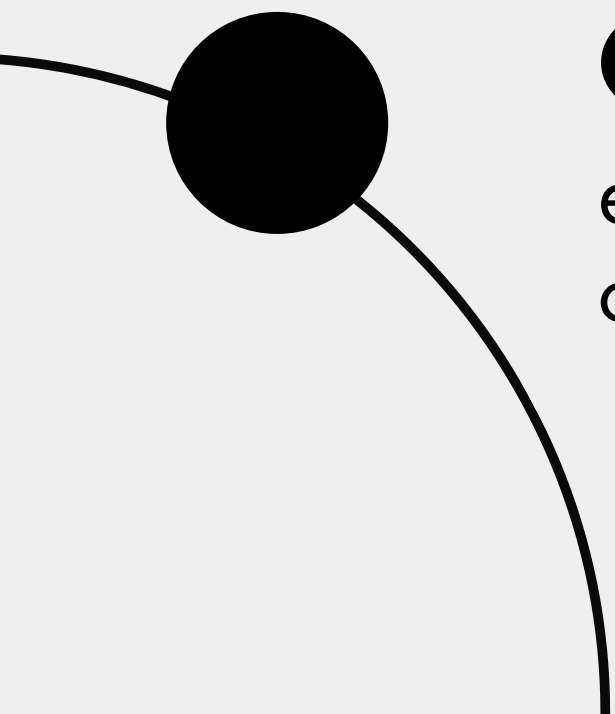
Pretending to be a figure of authority

Fear

Threatening consequences can override rational decision-making

Scarcity

Limited-time offers or exclusive deals create a fear of missing out.

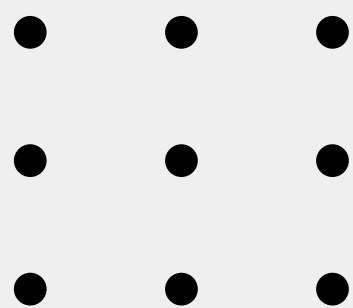


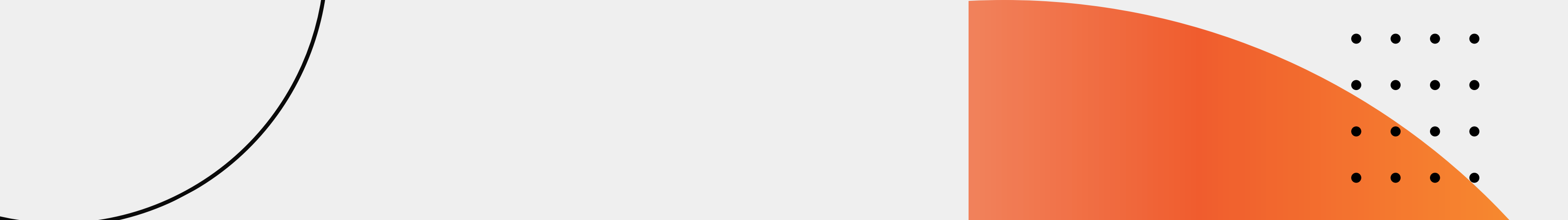
How to Protect Yourself

Verify identities: Always confirm who you're talking to before sharing information

Be skeptical: Question unsolicited requests, even if they seem urgent.

Educate others: Share knowledge about social engineering tactics with friends, family, and colleagues





Tools for Checking Personal Data

- Data breaches are common, and personal information (e.g., emails, passwords, credit card numbers) can be exposed.
 - Monitoring tools help you stay informed and take action if your data is compromised.
- 

Tools

Have I Been Pwned?

Check if your email or phone number has been involved in a data breach.

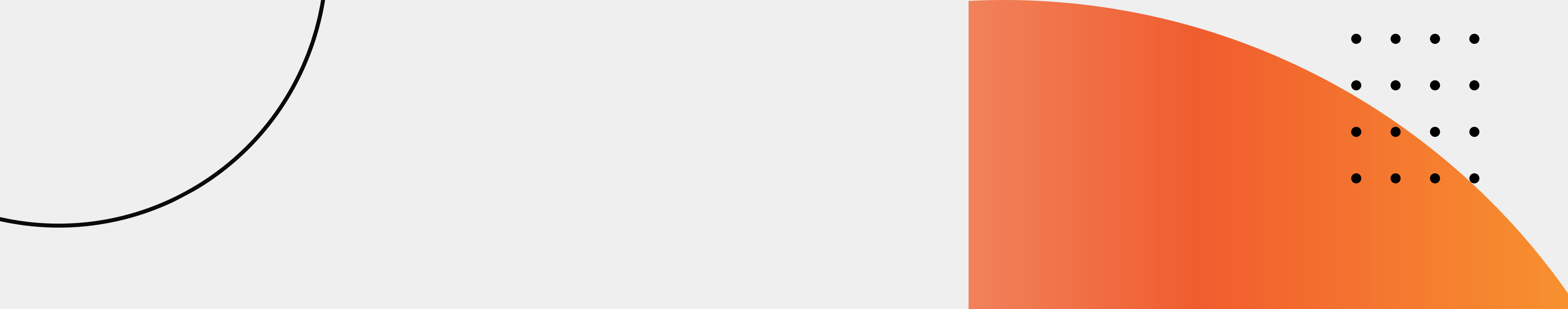
Google Security Checkup

Review and secure your Google account settings

Credit Monitoring Services

Tools like Credit Karma or Experian help monitor your credit report for suspicious activity.

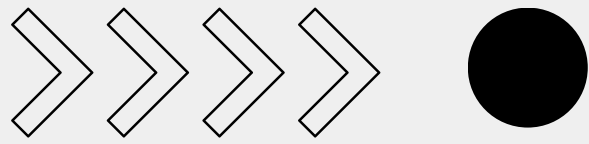
-
-
-
-
-
-



Encryption: Protecting Your Data

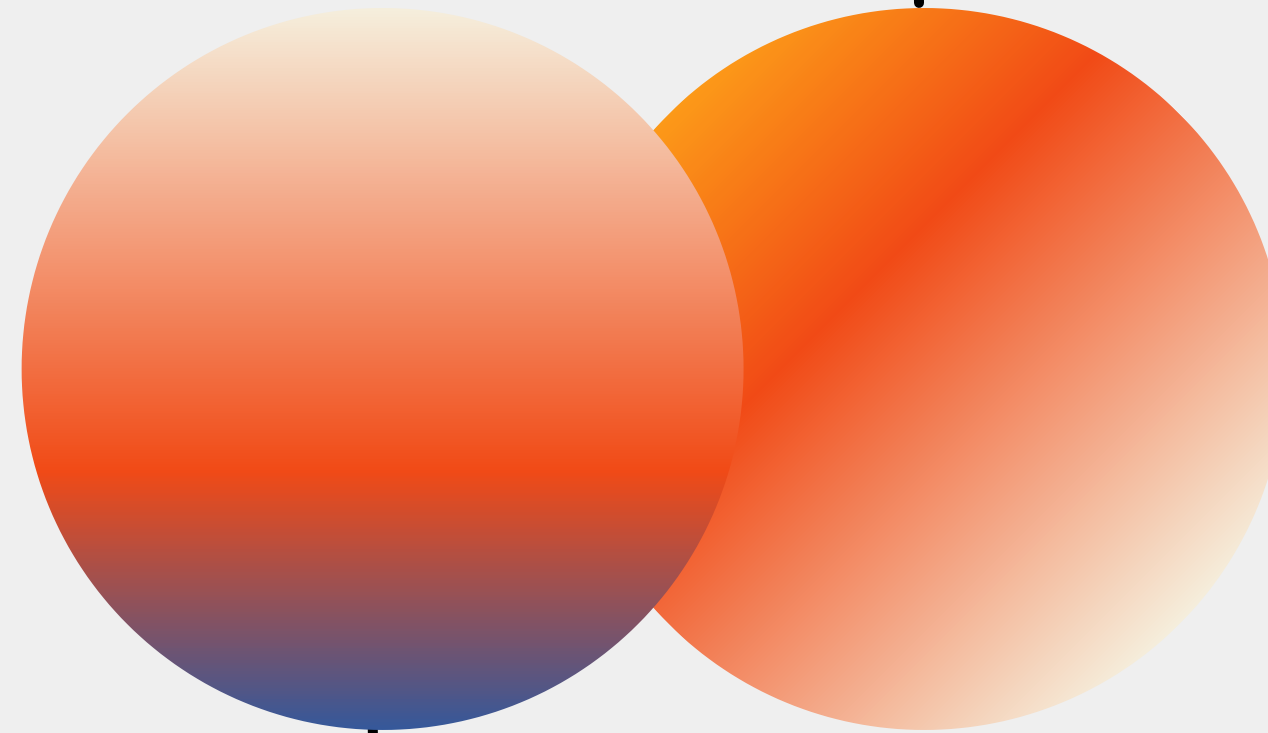
Encryption is the process of converting data into a coded format to prevent unauthorized access.





Symmetric encryption

Uses the same key to encrypt and decrypt data.



Asymmetric encryption

Uses a public key to encrypt data and a private key to decrypt it.

tips : Websites with `https://` encrypt the connection. Without it, attackers on public Wi-Fi can spy on what you type.

Where is Encryption Used?

Secure communication

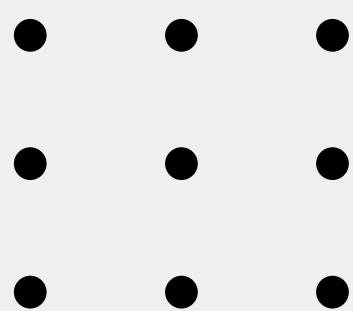
HTTPS websites, messaging apps (e.g., Signal, WhatsApp).

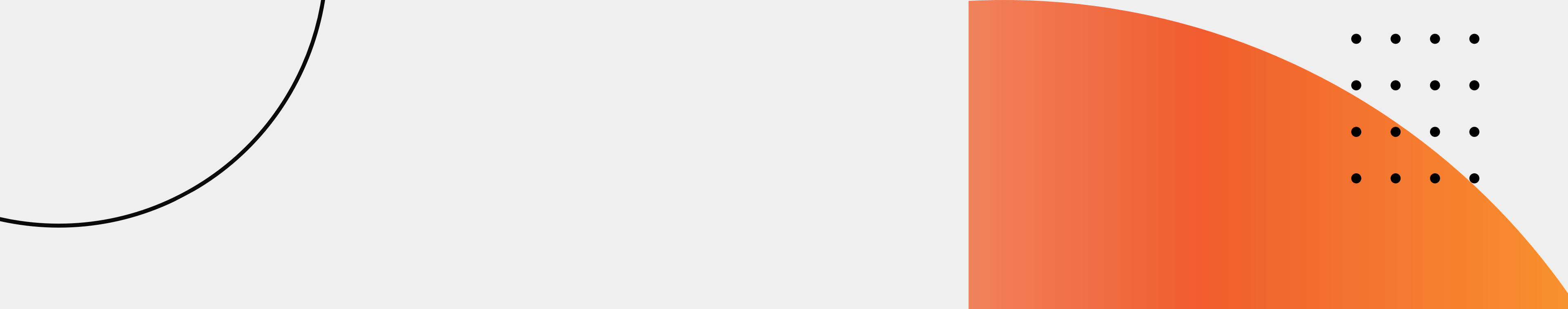
File encryption

Tools like BitLocker (Windows) or VeraCrypt (cross-platform) protect sensitive files.

Email encryption

Services like ProtonMail offer end-to-end encryption for emails.





Ransomware: Holding Data Hostage

Ransomware is malware that encrypts files and demands payment (usually in cryptocurrency) for their release



Ransomware

Backup your data

**Keep software
updated**

**Avoid suspicious
links/attachments**

**Use antivirus
software**



Ransomware

**Do not pay the
ransom**

**Disconnect from
the network**

Report the attack

**Restore from
backups**



End

Thank you

Do you have any questions?

