EMPLOYEE SECURITY PROGRAM

Cybersecurity Awareness Training

Spot the threat. Stop the breach. Protect the business — every single day.

KingSec 60-minute live session Designed for non-technical staff

What You'll Take Away Today

AGENDA

A practical hour — built around the decisions you make every day

01

Why this matters to you

The real business cost — and why attackers target people, not just computers

02

Recognise the threats

Phishing, BEC, ransomware and social engineering, in plain language

03

Build secure habits

Passwords, MFA, safe browsing, remote and mobile working

04

Respond with confidence

Exactly what to do in the first five minutes of an incident

Why Cybersecurity Is Everyone's Job

Small businesses are targeted on purpose — because defences are often weaker

95%

of breaches trace back to a human action: a click, a reply, a reused password

$4.45M

average cost of a single data breach worldwide (IBM, 2023)

1 in 3

small firms hit by a serious attack never fully recover from the disruption

The takeaway: Technology blocks most attacks automatically. The ones that get through are aimed at **people**. That makes you the most important part of the company's defence.

The Threats You'll Actually Meet

Six tactics behind almost every attack on a business like ours

Phishing

Fake messages that trick you into clicking, logging in, or paying

Business Email Compromise

A scammer poses as your boss or a supplier to redirect money

Ransomware

Your files are locked and held hostage until a ransom is paid

Social Engineering

Manipulating trust, in person or by phone, to gain access

Weak & Reused Passwords

The easiest door for an attacker to walk straight through

Unsecured Wi-Fi & Devices

Public networks and lost phones quietly leak company data

Phishing: The #1 Way Attackers Get In

A fake message from a 'trusted' source, designed to make you act fast

Criminals send a message that looks like it’s from your bank, a supplier, a courier, or even a colleague. One careless click can hand them the keys.

What they’re really after:

- Your username and password
- A money transfer to their account
- You opening an infected attachment
- Personal or company data they can sell

It works like fishing

The attacker casts thousands of fake 'baits' and only needs one person to take the hook.

Today, you learn not to bite.

It also arrives by SMS (smishing) and by phone call (vishing).

Anatomy of a Phishing Email

The kind of email a real employee received — every red flag marked

From: **support@hbl-secure-alert.com**

Subject: URGENT: Verify Your Account Now

Dear Valued Customer,

We detected SUSPICIOUS ACTIVITY on your account. It will be PERMANENTLY SUSPENDED in 24 hours unless you verify immediately.

http://hbl-verify-account-pk.xyz/login

HBL Customer Support

Wrong sender domain

Real HBL uses @hbl.com, never a look-alike

Manufactured urgency

'24 hours' and 'PERMANENTLY' rush you

Suspicious link

Hover first — a .xyz address is not a bank

Generic greeting

'Valued Customer' — your bank knows your name

Seven Red Flags in Every Phish

Spot any one of these and slow down — it’s probably a trap

1 **Urgency or threats**

"Act now or lose access" makes you skip checks

2 **Sender doesn’t match**

Display name says a brand; the address doesn’t

3 **Generic greeting**

"Dear Customer" instead of your real name

4 **Mismatched links**

Hover — the real URL won’t match the text

5 **Unexpected attachments**

An invoice or 'DHL notice' you never asked for

6 **Spelling & grammar slips**

Real organisations proofread their emails

7 **Asks for password or payment**

No legitimate company asks this by email

Business Email Compromise: The CEO Scam

BEC

The most expensive trick in the book — and it runs entirely on trust

An attacker impersonates an executive or a supplier and asks an employee to move money or share data — quietly and quickly.

1 · Research

They study your company on LinkedIn and the website to copy names, tone and the org chart.

2 · The Ask

"Hi Sana, I’m in a meeting. Please transfer Rs 250,000 to this vendor ASAP. Keep it confidential."

3 · The Loss

The staff member rushes to please the 'boss'. By the time anyone checks, the money is gone.

The rule: Any urgent or confidential money request, even from the CEO, gets verified by phone on a number you already have — not the one in the email.

Passwords: The Lock on the Front Door

Long and unique beats short and clever — every time

✕ DON'T

- Use your name, birthday or company name
- Reuse one password across many sites
- Use short passwords (under 12 characters)
- Share passwords over WhatsApp or email
- Write them on sticky notes at your desk

✓ DO

- Use a passphrase: RedLion$RunsFast22!
- Use a different password for every account
- Let a password manager remember them (Bitwarden)
- Turn on MFA wherever it's offered
- Change it at once if you suspect exposure

Multi-Factor Authentication (MFA)

A second lock that holds even if your password is stolen

MFA asks for two kinds of proof before letting anyone in. Even with your password, an attacker is stopped without the second factor — it blocks over 99% of automated attacks.

Something you know

Your password or PIN

Something you have

Your phone — an app code or tap-to-approve

Something you are

Your fingerprint or face

Turn it on today for: Email · Banking · Social media · Company systems · Cloud storage

Social Engineering: Hacking the Human

Attackers exploit politeness and trust — no computer skills required

THINK IT THROUGH

A confident stranger with a laptop bag and a company-looking ID tells reception he’s "from IT" and needs to access the office computers.

He’s friendly. He’s in a hurry.

Should reception let him in?

Answer: not without verifying. Real IT never minds being checked.

Vishing

Fake calls posing as IT, your bank, Easypaisa/JazzCash or a government office

Pretexting

A believable cover story (fake IT, courier) used to earn your trust

Shoulder surfing

Watching you type a password or PIN in a public place

Baiting

A 'lost' USB drive left out, hoping curiosity makes you plug it in

Safe Web Browsing

Your browser is a door to the company — keep it guarded

✓ SAFE HABITS

- Look for HTTPS and the padlock before you type anything
- Keep your browser and extensions updated
- Download software only from official sites
- Log out of accounts on shared computers
- Stick to company-approved tools and sites

× AVOID

- Pop-ups screaming your device has a virus
- Cracked or pirated software — it carries malware
- Unknown sites on work devices
- Saving passwords unprotected in the browser
- Clicking past browser security warnings

Note: HTTPS means the connection is private, not that the site is honest. Phishing sites use it too.

Working Remotely, Safely

REMOTE

Your home network is now part of the company's security

Secure your Wi-Fi

Use WPA2/WPA3 and change the default router password.

Use company devices

Keep work and personal accounts off the same device.

Connect to the VPN

If provided, always use it — it encrypts your traffic.

Lock your screen

Windows + L whenever you step away, even at home.

Mind your surroundings

No sensitive calls or screens in public view.

Report fast

Lost device or odd email? Tell IT immediately.

Mobile Device Security

Your phone holds as much company data as your laptop

✓ PROTECT YOUR PHONE

- Strong PIN or fingerprint / face unlock
- Auto-lock after 1 to 2 minutes
- Keep the OS and apps updated
- Install only from official app stores
- Turn on remote-wipe for loss or theft

× WATCH OUT FOR

- Fake banking / delivery apps
- Smishing — scam links sent by SMS
- Unknown public Wi-Fi hotspots
- Public USB charging (juice jacking)
- Apps demanding needless permissions

If Something Goes Wrong: Act Fast

The first five minutes decide how much damage is done

1

STOP

Don’t click anything else. Disconnect from the internet if you can.

2

REPORT

Tell your manager or IT contact right away. Speed limits the damage.

3

DOCUMENT

Note what you saw: sender, link, message. A screenshot helps.

4

COOPERATE

Work with IT. Don’t delete anything — it may be evidence.

Remember: There is no punishment for reporting a mistake. There is real damage from hiding one.

Your Daily Security Checklist

Small habits, repeated daily, are what actually keep us safe

- ☑ Lock your screen when you step away (Windows + L)
- ☑ Check the sender’s address before clicking any link
- ☑ Use your password manager — never reuse passwords
- ☑ Don’t join unknown Wi-Fi on work devices
- ☑ Report anything suspicious — even if you’re unsure
- ☑ Log out of accounts before you leave
- ☑ Install updates promptly — they close security gaps

Knowledge Check — Question 1 of 5

Pick the best answer — we'll discuss as a group

QUIZ

Q1. An email from 'CEO@company-pk-urgent.net' asks you to transfer money immediately. What do you do?

A Transfer it right away — it's the CEO

B Call the CEO on a number you already have to verify

C Reply to the email asking for more details

D Ignore and delete it without telling anyone

Knowledge Check — Question 2 of 5

Pick the best answer — we'll discuss as a group

QUIZ

Q2. Which of these is the strongest password?

A ahmed1990

B P@ssword1

C BlueSky$JumpsHigh22!

D 12345678

Knowledge Check — Question 3 of 5

Pick the best answer — we'll discuss as a group

QUIZ

Q3. You find a USB drive in the office car park. What's the safe move?

A Plug it into your computer to find the owner

B Hand it to your manager or IT contact, unopened

C Plug it into your personal phone instead

D Throw it in the bin

Knowledge Check — Question 4 of 5

Pick the best answer — we'll discuss as a group

QUIZ

Q4. What does MFA actually protect you from?

A Nothing — it's just extra hassle

B Malware, automatically

C Unauthorised access even when your password is stolen

D Spam emails

Knowledge Check — Question 5 of 5

Pick the best answer — we'll discuss as a group

QUIZ

Q5. You clicked a suspicious link. What's the best first step?

A Close the browser and hope nothing happened

B Restart and wait to see what happens

C Disconnect from the network and report it immediately

D Run a scan in the background and keep working

Three Habits That Protect Us All

If you remember nothing else from today, remember these

1

STOP & VERIFY

Before you click, open, or pay — pause and check. A 30-second call can save thousands.

2

PROTECT PASSWORDS

Long, unique passphrases. MFA on every important account. Let a manager do the remembering.

3

REPORT IMMEDIATELY

See something off? Say something. You're never in trouble for reporting, only for silence.

You are not the weakest link. Trained and alert, you are the company's strongest defence.

Questions & Answers

No question is too simple. Cybersecurity is a shared responsibility.

YOUR SECURITY CONTACTS

Report suspicious activity to: **Abdul Mannan / +9270-7271232 kingusecurity@gmail.com**

Forward phishing samples to: **kingusecurity@gmail.com**