Faysal Aziz

Phish-Savvy in a Day

Spot the Scam—Stay Safe

FA-0540 · one day

Cybersecurity

Introduction

Scammers don't take weekends off—and their emails, texts, and phone calls are getting better every year. Some even use AI to copy the way real companies talk, making it harder to tell what's real and what's fake.

This course is for everyday people—no tech skills needed—who want to stop falling victim to email scams and other phishing tricks. In just one day, you'll see real examples of scams, practice spotting the clues, and learn the habits that will keep you and your family safer online.

Your instructor has over 30 years of industry experience fighting cybercrime and will use **real, up-to-date scam examples** instead of boring theory.

Learning outcomes

By the end of this course, participants will be able to:

- Recognize the most common types of phishing attacks (email, text, phone, QR code).
- Spot at least **10 different warning signs** in scam messages.
- Safely inspect links, attachments, and sender addresses before interacting with them.
- Take safe, immediate action if they've clicked something suspicious.
- Build daily habits that reduce the risk of falling for scams.
- Confidently help friends and family identify and report phishing.

Prerequisites

- Basic ability to open and read an email or text message.

- Willingness to interact, ask questions, and try practice activities.
- No prior technical knowledge required.

Training outline

1. Section 1: Opening & Icebreaker

Setting the Stage — Why We Need to Be Phish-Savvy

- What phishing is and why it works.
- Stories of real victims and what happened.
- How phishing has evolved: from clumsy spam to AI-crafted scams.
- Why scammers target everyday people (and not just big companies).

Activity:

- *"Phish or Real?" Warm-Up Game*: Quick-fire slideshow—participants shout "Phish!" or "Real!" for each example. Discuss answers.

---

2. Section 2: Phishing 101: Anatomy and Evolution

How Scammers Trick the Brain

The psychology of scams:

  - Fear ("You'll lose access to your account").
  - Urgency ("Act in the next 5 minutes").
  - Greed ("You've won a prize").
  - Curiosity ("See who viewed your profile").
- How emotions make people click before thinking.
- Overview of phishing types: classic, spear phishing, AI-enhanced, and QR (quishing) attacks.
- The evolution of phishing: from broken English to AI-generated, perfectly worded messages.
- Examination of real incidents: dissecting headline-making attacks from recent months.

Simulation:

- Fake “bank” email is shown—participants identify which phrases are trying to trigger emotions.

Anatomy of a Scam Message

Breaking down a real phishing email:

- Suspicious sender address.
- Mismatched links.
- Odd language or formatting.
- Unexpected attachments.

- Differences between sloppy scams and professional-looking fakes.

Hands-On:

- Participants work in pairs with printed fake emails—highlight the suspicious parts.

---

3. Section 3: Spotting Red Flags

Safe Link & Attachment Checks

- How to hover over links (mouse and mobile).
- Recognizing shortened URLs.
- Dangerous file types: .exe, .zip, .scr, and why they’re risky.

Activity:

- Instructor shows a safe, controlled “sandbox” of fake links—participants practice hovering and reading addresses without clicking.

Types of Phishing to Watch Out For

- **Email phishing** — the most common.
- **Smishing** — scam texts with bad links.
- **Vishing** — fake calls pretending to be from banks or government.
- **Quishing** — QR code scams leading to fake sites.

- **Business email compromise** — even work emails can be faked.

Activity:

- Matching game—participants match the scam type with the example.

What to Do If You Spot (or Fall For) a Scam

- How to report an email in Gmail, Outlook, or on a phone.
- Who to contact first (bank, email provider, police report if needed).
- Changing passwords immediately.
- Checking for signs of identity theft.

Simulation:

- A "You clicked it" roleplay—participants follow a checklist to recover safely.

Building Long-Term Safety Habits

- Slow down—stop before you click.
- Keep software and devices updated.
- Use spam filters and two-factor authentication.
- Unique passwords for each account.
- Be careful on public Wi-Fi.

Group Brainstorm:

- Participants make a personal "Phishing Safety Pledge" with 3 habits they'll keep.

---

4. Section 4: Gamified Phishing Simulation

The Family & Friends Multiplier

- Why scammers love targeting older relatives and kids.
- Simple tips to teach loved ones.
- How to forward suspicious emails for a second opinion.

Roleplay:

- “Explaining it to Grandma”—practice teaching someone less tech-savvy.

---

5. Section 5: Advanced Tactics and Defense Layers

Final Practice Challenge

- Social engineering: Pretexting, urgency, and impersonation.
- Deep dive on quishing (QR-code phishing) and emerging threats.
- Defending your inbox: Multi-factor authentication, email security protocols (SPF/DKIM/DMARC), and modern AI-driven filtering solutions.
- Best practices: Verifying requests, using independent confirmation channels, and reporting suspicious emails.
  A timed challenge with 10 mixed real and fake emails/texts.
- Participants work individually, then review together.
- Instructor explains tricky examples.

Wrap-Up & Resources

- Recap of the top red flags.
- Printable “Phish-Savvy Quick Guide” to take home.
- Where to find safe online scam-reporting tools.

© 2026 Faysal Aziz · Kuala Lumpur