END-USER GUIDE

BullPhish ID

Your Security Awareness Training Program

This guide walks you through your role in BullPhish ID — understanding phishing simulations, completing training, and staying secure.

90%	85%	80+
of attacks start with phishing	click rate reduction after training	simulation kits available

Degarmo Technologies | degarmo.tech | July 2026

WHY THIS PROGRAM EXISTS

Your Inbox Is the Target

Understanding why phishing training matters for you and your organization.

WHAT IS BULLPHISH ID?

BullPhish ID is a security awareness training platform that keeps you informed, prepared, and protected against phishing attacks. Your organization has enrolled you in this program because phishing is the #1 way cybercriminals gain access to business systems — and training is the most effective defense.

WHY YOU MIGHT RECEIVE A SIMULATED PHISHING EMAIL

Periodically, you may receive realistic-looking phishing test emails sent by our security team through BullPhish ID. These are not real attacks — they are controlled tests designed to help you practice recognizing phishing without real risk.

What happens when you click:

If you click a simulated phishing link, you will see a "Teachable Moment" page explaining what you missed and why it matters. You may also be automatically enrolled in a short training course. This is not a punishment — it is how the training is designed to work.

Important: This Is a Safe Environment

No real harm comes from clicking a test email. The simulations are designed to teach, not to penalize. Every employee who completes the program becomes better at protecting themselves and the organization.

THE THREE THINGS YOU NEED TO KNOW

1. You Will Be Tested

You will receive realistic phishing simulation emails. Treat every unexpected email as potentially suspicious — even ones that look familiar.

2. Clicking Has Consequences

If you click a simulated phishing link, you will be enrolled in a training course. The course takes 5–15 minutes and is engaging video-based content.

3. You Can Report Suspicious Emails

If you receive an email that looks suspicious — test or real — report it using your email client's report phishing button. You will never be penalized for reporting.

4. Progress Is Tracked

Your training completion and simulation results are tracked by your organization's security team to measure the program's effectiveness and identify where additional help is needed.

RECOGNIZING PHISHING

How to Spot a Phishing Email

6 red flags every employee should know before opening a link or attachment.

THE 6 RED FLAGS

Suspicious Sender Address

Check the full email address, not just the display name. "Microsoft" as the name but "micros0ft-alerts.com" as the domain is a giveaway. Look for misspellings, hyphens, and wrong domain extensions.

Urgent or Threatening Tone

Phishing emails create urgency: "Your account will be suspended in 24 hours." Legitimate services rarely threaten immediate action without prior notice. Urgency is a pressure tactic designed to bypass your judgment.

Suspicious Links

Hover over any link before clicking. If the URL doesn't match the company it claims to be from, do not click. Look for extra words, numbers, or odd domains like "microsoft-login.support.com".

Unexpected Attachments

Never open an attachment you weren't expecting — even from someone you know. Attachments can contain malware that activates the moment you open the file.

Generic Greetings

"Dear Customer" or "Dear User" instead of your name is a sign of a mass phishing campaign. Legitimate companies you do business with typically use your name.

Requests for Credentials or Personal Data

No legitimate service will ever ask you to provide your password via email. If you receive a login page link in an email, go directly to the website by typing the address instead.

WHEN IN DOUBT — DON'T CLICK. REPORT.

If an email feels wrong, trust that instinct. You will never get in trouble for being cautious. Use the Report Phishing button in your email client, and our security team will review the message.

YOUR TRAINING

Completing Your Security Awareness Training

Short, engaging courses that build real skills. Here is what to expect.

HOW TRAINING IS ASSIGNED

You may be assigned training in two ways: (1) automatically, if you clicked a simulated phishing email, or (2) proactively, as part of your organization's scheduled security awareness program. Either way, you will receive an email notification with a link to your training portal.

WHAT YOUR TRAINING PORTAL LOOKS LIKE

Your white-labeled training portal shows all assigned courses, their due dates, and your completion status. Courses range from 5 to 20 minutes each and feature animated video content followed by a short quiz.

Video-Based Learning

All courses are animated and narrated — no dense reading required. Content is designed to be engaging and immediately applicable to your daily work habits.

Comprehension Quiz

Each course ends with a short quiz to confirm you understood the key concepts. The quiz is not a trick — it reinforces the most important points from the video.

Certificate of Completion

When you complete a course, a completion record is automatically saved. This is used by your organization for compliance documentation and audit evidence.

Reminder Emails

If you have an incomplete course, you will receive automatic reminder emails before the due date. Complete your training early to avoid deadline pressure.

QUICK REFERENCE: TRAINING TIPS

- ■ Complete your training within the assigned timeframe shown in the portal.
- ■ Courses can be paused and resumed — you do not have to complete them in one sitting.
- ■ If you have technical issues accessing the portal, contact your IT team or Degarmo Technologies.
- ■ All training is available in 8 languages — contact your administrator to change your language preference.

Questions? We're Here.

If you receive a suspicious email, are unsure about a simulated phishing test result, or have trouble accessing your training portal, contact Degarmo Technologies.

- **Same-day support available**
- **Email, phone, and portal support**

Visit degarmo.tech | Oklahoma City, OK | Veteran-Owned MSSP