



Congratulations!

You're taking the next step  
in protecting your organization from **cyber crime**.

**Security Awareness Training** helps keep your organization and your team safe from social engineering attacks, like phishing. Your program teaches technical and behavioral solutions and provides you with proof to share with regulators, auditors and partners.

With this Cybersecurity Training program, you will:

- Reduce your risk of a breach.
- Have proof of Cybersecurity Training for compliance purposes.
- Help you satisfy cyber insurer requirements.
- Preserve your hard-won reputation.

## Why is Cybersecurity Training so important?

Cybercrime is big business. The facts about security breaches are alarming:

- \$4.24 million average cost of a cybersecurity breach.<sup>1</sup>
- Average downtime per ransomware attack is 21 days.<sup>2</sup>
- Reputation damage can lower business valuation by 25%.<sup>3</sup>
- 15% increase in cybercrime every year.
- Human error is the primary way in for cyber attackers .
- Small- and medium-sized businesses are just as likely to be targeted as enterprises.
- Employees at all levels are targeted for information, not just executives.

1.<https://www.ibm.com/security/data-breach>

2.<https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020>

3.<https://www.aon.com/getmedia/2882e8b3-2aa0-4726-9efa-005af9176496/Aon-Pentland-Analytics-Reputation-Report-2018-07-18.pdf>

# Employee Expectations

## Part One: [Training Modules](#)

### Effortless Enrollment

Employees are automatically enrolled in the program, without any further effort on your part. Each employee receives email invitations when it's time to take training courses.

### Focused Content

The courses are designed to be focused and to-the-point, taking 5-10 minutes each.

### Effective Evaluation

Your employees will take a short quiz at the end of each module and must record a passing grade in order to progress to the next course.

### Automated Reminder Emails

We send email reminders so that you don't have to. These reminders include a link for training and go out to each employee who has not yet finished the current course.

### Immediate Feedback

Users receive real-time feedback on their performance. For each incorrect answer, they receive an explanation of the secure action or behavior.

## Part Two: [Simulated Phishing](#)

### Ongoing Behavior Modification

Every user receives a simulated phishing attack each month, varied in content and timing for all. If a user falls for one of these attacks, they'll receive immediate feedback and a reminder the following morning.

### High-Risk User Targeting

Users who click on phishing emails are automatically retargeted for additional simulated phishing. This highlights and remediates the most vulnerable.

## What additional benefits does your company receive?

The program administrator will receive regular updates regarding employee performance on the training modules. This information helps:

- Ensure your company's executive team has visibility regarding the state of cybersecurity knowledge and practices within your organization.
- Demonstrate compliance with relevant standards.
- Reduce the risk that your organization will be affected by a cybersecurity breach.
- Satisfy cyber insurance requirements.
- Identify and remediate unsafe employees and behaviors across the organization.

Best of all, it's easy. All of the set-up and administration of your Cybersecurity Training is handled automatically.

---

## What does success look like?

With cybersecurity, even one mistake can cost millions. With that in mind, success in Cybersecurity Training is defined by each employee:

- ✓ Completing each course with a passing grade.
- ✓ Passing the real world phishing simulations.
- ✓ Maintaining their safe behaviors as threats and training evolve.

