



## Click Thinking Interactive Training Catalog Rollout Guide

Available in the October 2023 Click Thinking bundle in the Content Center.

**Catalog and Rollout Guide**  
Click Thinking Interactive Training

Click Thinking Interactive Training is perfect for Cybersecurity Awareness Month or any time of year. Packed with engaging videos, games and infographics, they make training fast, fun and easy to implement!

**The Click Thinking Interactive Training Collection**

- CT1 Phishing Awareness** (10 minutes) - Click Thinking Phishing goes beyond the standard "don't click suspicious links" advice, showing how a single click can lead to a data breach or ransomware attack. Includes a simulated phishing email and a "Phishing 101" infographic.
- CT2 Passwords and Multi-Factor Authentication** (10 minutes) - Click Thinking Passwords goes beyond the standard "use strong passwords" advice, showing how a single password can lead to a data breach or ransomware attack. Includes a simulated password reset and a "Password 101" infographic.
- CT3 Personal Cybersecurity** (10 minutes) - Click Thinking Personal Cybersecurity goes beyond the standard "don't click suspicious links" advice, showing how a single click can lead to a data breach or ransomware attack. Includes a simulated phishing email and a "Personal Cybersecurity 101" infographic.
- CT4 Professional Cybersecurity** (10 minutes) - Click Thinking Professional Cybersecurity goes beyond the standard "don't click suspicious links" advice, showing how a single click can lead to a data breach or ransomware attack. Includes a simulated phishing email and a "Professional Cybersecurity 101" infographic.
- CT5 Basic Attack Techniques** (10 minutes) - Click Thinking Basic Attack Techniques goes beyond the standard "don't click suspicious links" advice, showing how a single click can lead to a data breach or ransomware attack. Includes a simulated phishing email and a "Basic Attack Techniques 101" infographic.
- CT6 Advanced Attack Techniques** (10 minutes) - Click Thinking Advanced Attack Techniques goes beyond the standard "don't click suspicious links" advice, showing how a single click can lead to a data breach or ransomware attack. Includes a simulated phishing email and a "Advanced Attack Techniques 101" infographic.
- CT7 Relying Safe Behaviors** (10 minutes) - Click Thinking Relying Safe Behaviors goes beyond the standard "don't click suspicious links" advice, showing how a single click can lead to a data breach or ransomware attack. Includes a simulated phishing email and a "Relying Safe Behaviors 101" infographic.
- CT8 Hybrid Work Security** (10 minutes) - Click Thinking Hybrid Work Security goes beyond the standard "don't click suspicious links" advice, showing how a single click can lead to a data breach or ransomware attack. Includes a simulated phishing email and a "Hybrid Work Security 101" infographic.
- CT9 Advanced Data Security** (10 minutes) - Click Thinking Advanced Data Security goes beyond the standard "don't click suspicious links" advice, showing how a single click can lead to a data breach or ransomware attack. Includes a simulated phishing email and a "Advanced Data Security 101" infographic.
- CT10 Advanced Personal Cybersecurity** (10 minutes) - Click Thinking Advanced Personal Cybersecurity goes beyond the standard "don't click suspicious links" advice, showing how a single click can lead to a data breach or ransomware attack. Includes a simulated phishing email and a "Advanced Personal Cybersecurity 101" infographic.
- CT11 Advanced Personal Cybersecurity** (10 minutes) - Click Thinking Advanced Personal Cybersecurity goes beyond the standard "don't click suspicious links" advice, showing how a single click can lead to a data breach or ransomware attack. Includes a simulated phishing email and a "Advanced Personal Cybersecurity 101" infographic.

Please see the next page for a comprehensive rollout guide and suggested implementation steps to make the most of this curriculum.

**Catalog and Rollout Guide**  
Click Thinking Interactive Training

Click Thinking Interactive Training is perfect for Cybersecurity Awareness Month or any time of year. Packed with engaging videos, games and infographics, they make training fast, fun and easy to implement!

**Getting Started**

- Review Click Thinking Interactive Training for a comprehensive overview of the training plan.
- Consider a comprehensive annual subject that includes essential topics for the entire year. Put a **hand-drawn note** in the subject **plan provided**.
- Consider Click Thinking Interactive Training as a core component of your training plan. There's no right or wrong time for Click Thinking Interactive Training. Start when you can, even if it's just for a few minutes a week.
- Implement Click Thinking Interactive Training on a regular basis with additional material available in the content center, including infographics, worksheets, and even conversational training modules.
- Personalized messages to each of your employees, emphasizing the fact that each module can be viewed in less than 10 minutes.
- Designed for the frontline, on-the-go employees, Click Thinking Interactive Training can be easily completed on mobile devices as it can be on a company desktop or laptop.

**Proposed Monthly Rollout Plan**

MOCT01	MOCT02	MOCT03
MOCT04	MOCT05	MOCT06
MOCT07	MOCT08	MOCT09
MOCT10	MOCT11	MOCT12

**Quarterly Emphasis: Understanding Fundamentals**  
Builds a solid foundation of knowledge with training that emphasizes fundamental information security topics and best practices.

**Quarterly Emphasis: Securing the Organization**  
Fortifies front-line employees with the knowledge they need to protect your organization against common and sophisticated cyber attacks.

**Quarterly Emphasis: Beyond the Workplace**  
Explores threats that can compromise individuals in their personal or hybrid work spaces while providing insights that protect them.

**Quarterly Emphasis: Protecting Data**  
Provides an in-depth look at the causes and impacts of data breaches, emphasizing everyone's role in preventing them.