FONDAZIONE BRUNO KESSLER
MAGAZINE

When phishing becomes a lesson

June 24, 2026

HoneyPeople's journey across research, schools, and communities

There comes a moment during a phishing attack when even the most self-confident people begin to doubt themselves. A seemingly legitimate email, a convincingly written message, an urgent request: it takes very little to turn a cyberattack into something deeply human.

This awareness inspired the educational initiative developed by Fondazione Bruno Kessler around HoneyPeople, the cyber deception tool created by the DAISY unit at FBK's Center for Cybersecurity, in collaboration with the University of Trento. Originally created as a research tool to study social engineering and attacker behavior, HoneyPeople uses Generative Artificial Intelligence to simulate realistic and secure email interactions. Over time, the project has evolved into an effective training and awareness program capable of engaging different audiences, including citizens, high school students, and international students from a variety of disciplines.

The goal is not only to explain what **phishing** is, but to provide a concrete and realistic experience that shows how attackers exploit emotions, digital habits, and psychological mechanisms far more often than technical vulnerabilities.

Phishing today: an increasingly human problem

Phishing has evolved rapidly in recent years. While many online scams were once easy to recognize, today's attacks have become more credible, personalized, and sophisticated, thanks in part to the spread of generative artificial intelligence.

Social engineering techniques exploit urgency, trust, fear, and curiosity to persuade people to click on malicious links, share sensitive information, or perform risky actions. In this context, the human factor has increasingly become the primary entry point for attacks.

For this reason, **cybersecurity awareness** can no longer be limited to theoretical explanations or abstract guidelines. Instead, it is essential to create practical and engaging experiences that demonstrate how attacks work and what warning signs can help identify them. At the European level as well, strategies and regulations such as the NIS2 Directive are placing growing emphasis on training and awareness, recognizing the human factor as one of the central elements of digital security.

From research to outreach: the role of HoneyPeople

HoneyPeople was developed within the field of cyber deception, an approach that uses credible environments and interactions—also generated through AI and monitored by the system itself—to slow down, observe, and better understand attacker behavior. The system leverages the same social engineering techniques used in real phishing campaigns, creating digital identities and plausible scenarios with which attackers can interact. This allows researchers to study the dynamics, strategies, and methods used throughout the different stages of an attack.

Designed to reconstruct and analyze phishing-related attack chains, the system has also proven over time to be a particularly effective tool for education and outreach.
Through realistic simulations, interactive scenarios, and gamification-based activities, HoneyPeople allows participants to take on the role of the attacker and understand complex concepts through experiences that remain accessible even to people without specialized technical skills.

This **experiential approach** has proven especially effective in engaging participants and making the mechanisms behind phishing and social engineering more tangible and understandable. After all, what better way to learn how to defend yourself than by seeing firsthand what makes an attack credible and effective?

Understanding risk through experience: a journey across communities, schools, and universities

The activities developed with HoneyPeople have been tested in a wide range of settings, involving citizens, high school students, and international participants from multidisciplinary backgrounds.

The first public experience took place during Research Night 2025, where participants were invited to step into the role of an attacker through a series of progressive challenges inspired by Capture The Flag (CTF) competitions. The activity demonstrated how seemingly harmless information can be used to build targeted and convincing attacks, while also encouraging direct interaction with researchers and the sharing of personal experiences related to scams and online deception attempts.

The experience was later adapted to the school environment through collaboration with the Scholars and PhD Program Unit and Galileo Galilei High School in Trento. With the support of teachers, who helped tailor the content and interaction methods to the needs of different classes, the activities were integrated with in-depth sessions on phishing, social engineering, and the impact of Artificial Intelligence, followed by practical exercises focused on analyzing suspicious emails. Many students, initially convinced that they could easily recognize an attack, discovered how difficult it can be to distinguish authentic communications from carefully crafted fraudulent messages.

The same approach was later offered to approximately 60 international students participating in the MERIT project. Despite the participants' diverse academic backgrounds, the activities highlighted how phishing, online manipulation, and digital awareness are cross-cutting issues that affect anyone working in increasingly digitalized environments.

Across all these experiences, one common theme emerged: learning is more effective when people are directly involved in realistic scenarios that allow them to observe, understand, and experience firsthand the mechanisms behind cyberattacks.

Beyond technology: building awareness

The experiences developed through HoneyPeople demonstrate how tools born from research can have a concrete impact beyond the laboratory, becoming opportunities for education, outreach, and engagement.

In a context where cyberattacks are becoming increasingly credible and personalized thanks to Artificial Intelligence, technology alone is not enough. What is needed is awareness, critical thinking, and the ability to recognize manipulative dynamics that rely primarily on human behavior. For this reason, alongside traditional regulations, guidelines, and training programs, it is becoming increasingly important to experiment with innovative educational approaches that actively engage people and transform cybersecurity from an abstract concept into a tangible experience.

The activities carried out with HoneyPeople have shown how gamification, direct interaction, and realistic scenario simulations can make topics often perceived as complex or distant from everyday life more accessible and memorable. They also represent a starting point for developing even more awareness-oriented cybersecurity tools, using Artificial Intelligence to create personalized learning paths, dynamic simulations, and interactive challenges that support people in acquiring the skills needed to face the digital threats of today and tomorrow.

Daniele Santoro, Claudio Facchinetti, Domenico Siracusa, Matteo Franzil, Adriano Patton, Valentina Pasqualino, and Andrea Palmieri participated in the activities.

PERMALINK

https://magazine.fbk.eu/en/news/quando-il-phishing-diventa-una-lezione/

TAGS

- #artificialintelligence
- #attacchi informatici
- #cyber deception
- #cybersecurity
- #cybersecurity awareness
- #daisy
- #formazione
- #giovani
- #HoneyPeople
- #ia generativa
- #Merit
- #NIS2
- #phishing
- #social engineering
- #studenti

RELATED MEDIA

- HoneyPeople: https://daisy.fbk.eu/tools/HoneyPeople/
- Guida rapida per comprendere le minacce digitali e le strategie di difesa: https://magazine.fbk.eu/wp-content/uploads/2026/06/Phishing-AI-e-larte-dellinganno.pdf

AUTHORS

- Daniele Santoro