

CYBERSECURITY

ETHICAL HACKING

PENETRATION TESTING

TRAINING



Phishing & Smishing

Simulated campaigns and training turn human risk into a stronger line of defence



OBJECTIVE

Measure and reduce risk before a message becomes an incident

Phishing, smishing and vishing exploit trust, urgency and routine to bypass technical controls.

Simulations reveal real behaviour and guide targeted training without blaming people.

METHOD

Prepare, simulate and train through a **measurable cycle**

Design

We define targets, pretext, channel, difficulty and metrics with privacy in mind.

Campaign

Realistic messages are sent safely without collecting real credentials.

Training

Immediate feedback and targeted content turn mistakes into learning.

DELIVERY

Email, SMS and voice scenarios **aligned with the business**

Campaigns reproduce internal communications, suppliers, cloud services and relevant themes.

Targets and frequency are segmented by role, exposure and previous results.

Repeated campaigns measure improvement and reinforce rapid reporting.





KEY STRENGTHS

Realism, respect for people and practical learning

Safety

Landing pages and data collection avoid exposing sensitive information.

Relevance

Pretexts and difficulty are calibrated to recipients' day-to-day work.

Growth

Metrics guide training and controls rather than punishment.



OUTPUT

Clear metrics on behaviour and reporting capability

Interaction rate by channel, group and scenario.

Reporting rate and time to alert security teams.

Pattern analysis identifying drivers of human risk.

Training plan focused on observed behaviour.

Let's **HACK** together



ISGroup
Information Security

CF e P.IVA 04164220230
www.isgroup.it

BOOK A MEETING
sales@isgroup.it
+39 045 4853232