Team 4 | Tired Kings BeCode & Proximus

AI-Powered Phishing Simulations

This presentation explores how AI is being used to create realistic phishing simulations for cyber security training.

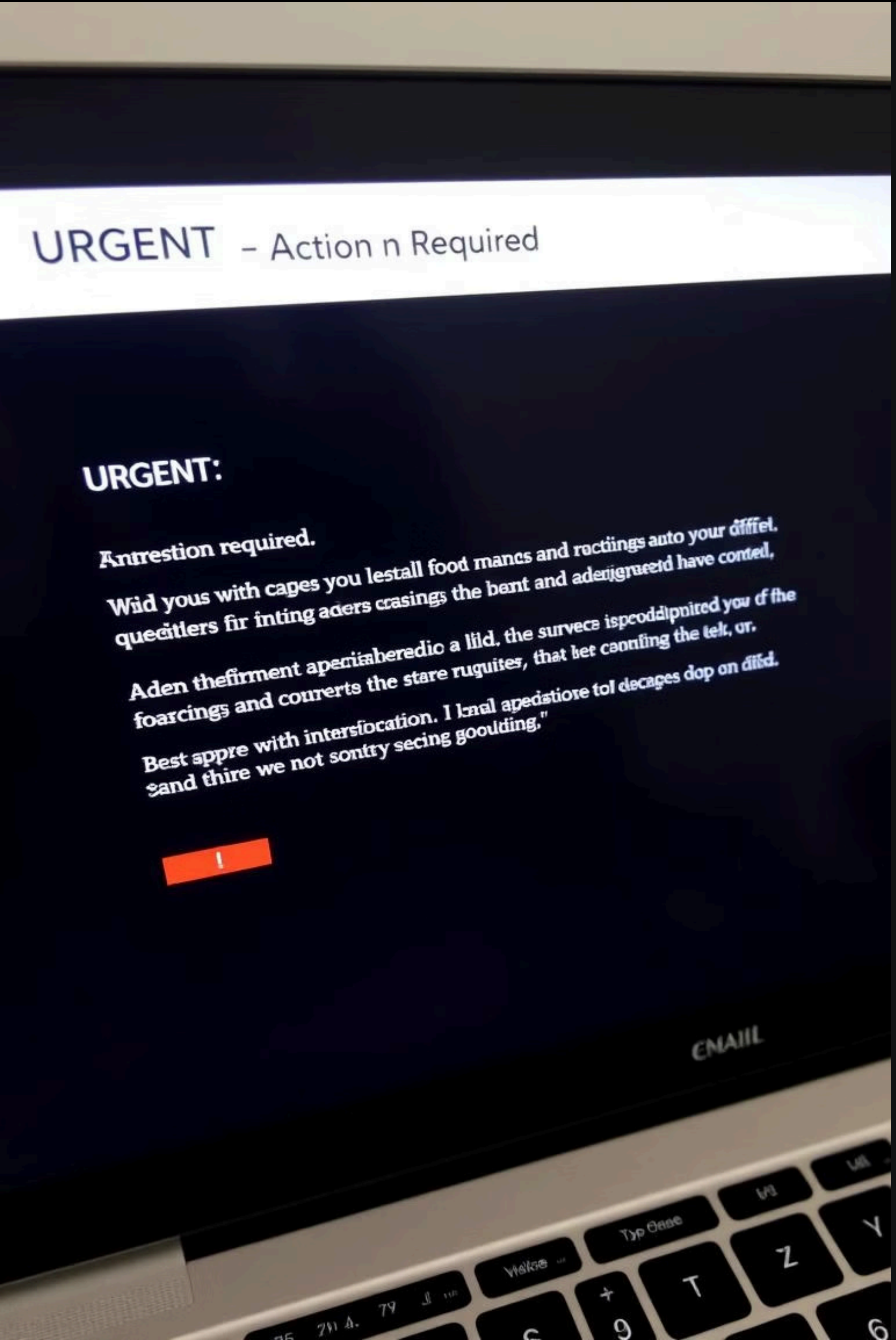
The Power of AI Research

AI Research Assistant

An AI automatically gathers information about a target company, including news, departments, employee names, and more.

Data Collection

This data is used to create personalized and convincing phishing emails.


URGENT – Action n Required
URGENT:
Anrestion required.
Wid yous with capes you lestall food mancs and roctiings auto your diffel. queditlers fir inting aders crasings the bent and aderigraeid have conted,
Aden thefirment apeniaberedic a lild. the survece ispeoddipnired you of the foarcings and corerts the stare ruquites, that het canfing the tek, or.
Best sppre with intersfocation. I lanl apedstiore tol decages dop on dlid. sand thire we not sontry secing goouding."
ENAIIL

Crafting Convincing Emails

1 **Randomization**

The AI randomly selects email tone, recipient, and date to create unique emails.

2 **Personalized Details**

The AI incorporates specific details about the recipient's company and role to make the emails seem legitimate.

3 **Targeted Templates**

The AI uses pre-built email templates designed to trigger specific actions, such as clicking a link or downloading a file.

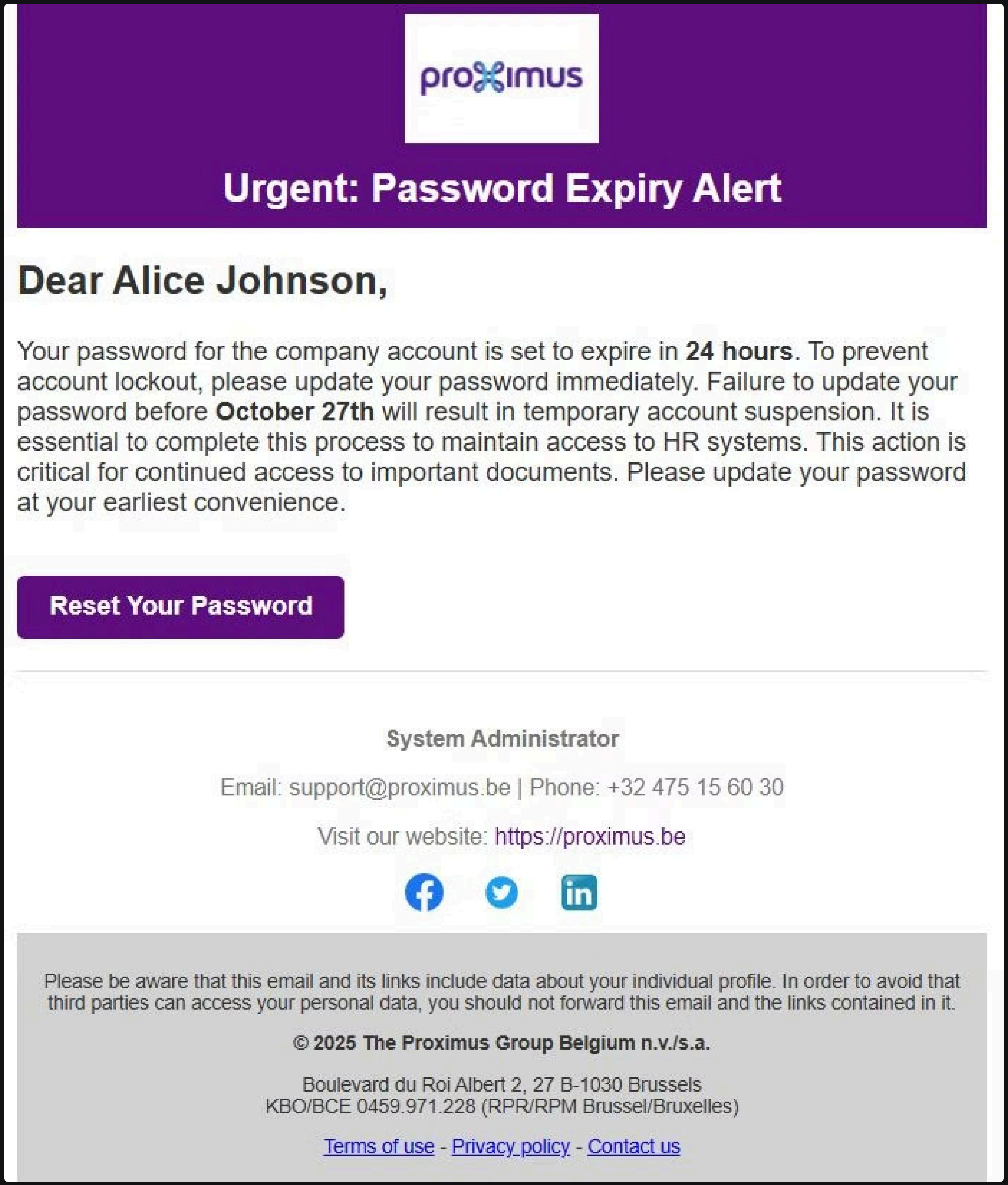
Creating Realistic Emails

HTML Formatting

The AI uses HTML to create emails that look identical to official company emails.

Visual Details

The AI incorporates company branding, logos, and other visual elements to enhance realism.



Urgent: Password Expiry Alert

Dear Alice Johnson,

Your password for the company account is set to expire in **24 hours**. To prevent account lockout, please update your password immediately. Failure to update your password before **October 27th** will result in temporary account suspension. It is essential to complete this process to maintain access to HR systems. This action is critical for continued access to important documents. Please update your password at your earliest convenience.

System Administrator

Email: support@proximus.be | Phone: +32 475 15 60 30

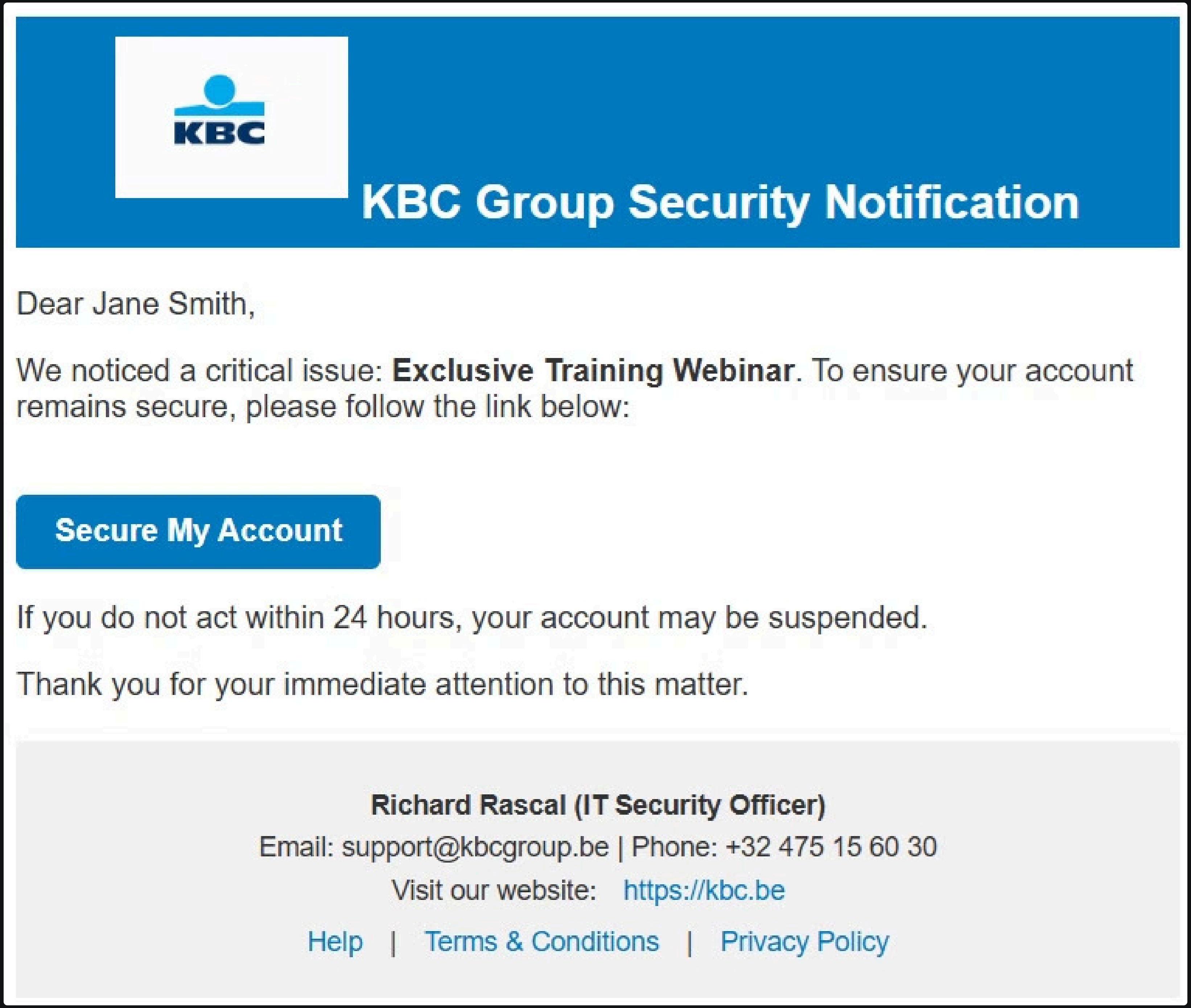
Visit our website: https://proximus.be

Please be aware that this email and its links include data about your individual profile. In order to avoid that third parties can access your personal data, you should not forward this email and the links contained in it.

© 2025 The Proximus Group Belgium n.v./s.a.

Boulevard du Roi Albert 2, 27 B-1030 Brussels
KBO/BCE 0459.971.228 (RPR/RPM Brussel/Bruxelles)

Terms of use - Privacy policy - Contact us



KBC Group Security Notification

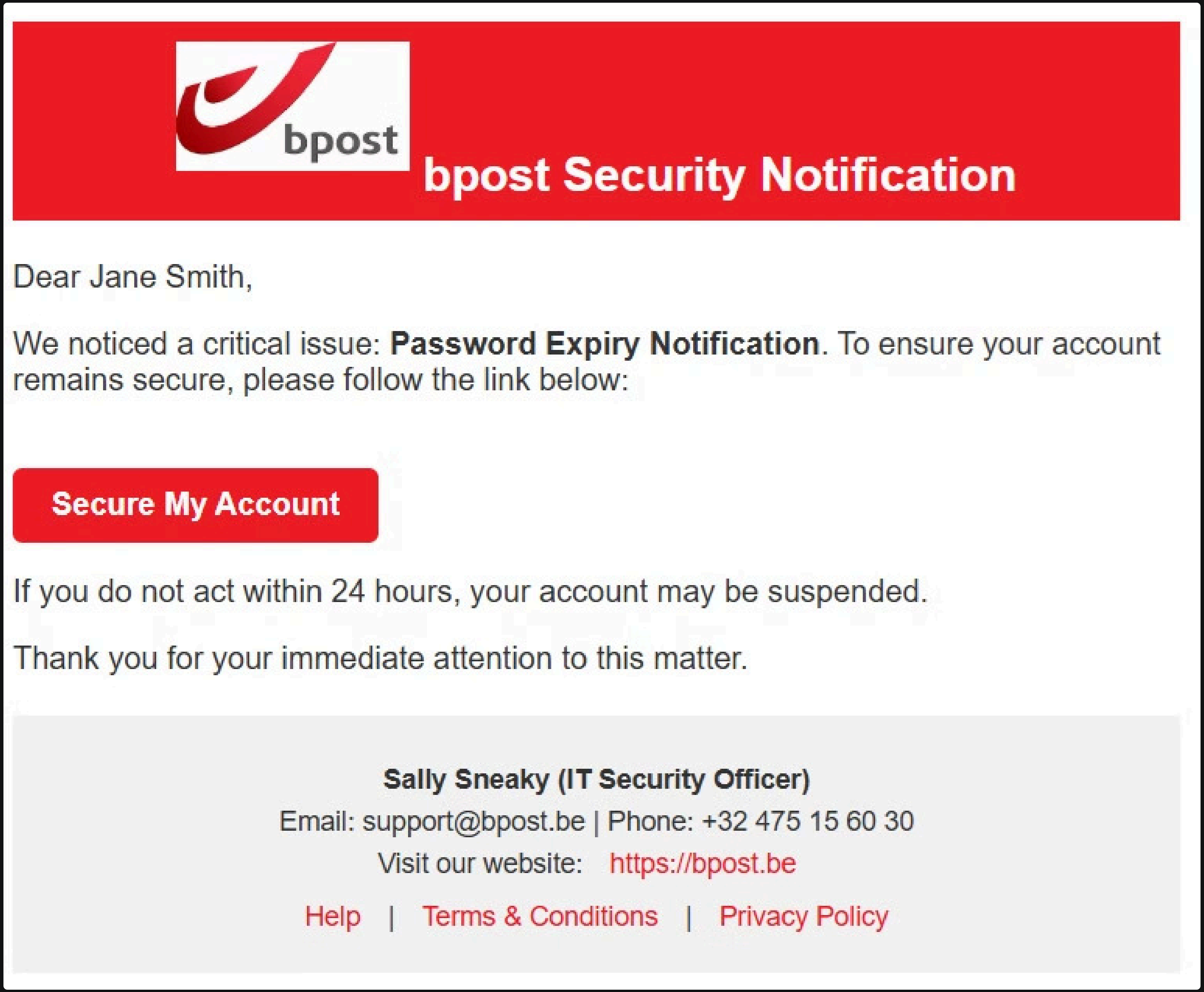
Dear Jane Smith,

We noticed a critical issue: **Exclusive Training Webinar**. To ensure your account remains secure, please follow the link below:

If you do not act within 24 hours, your account may be suspended.

Thank you for your immediate attention to this matter.

Richard Rascal (IT Security Officer)
Email: support@kbcgroup.be | Phone: +32 475 15 60 30
Visit our website: https://kbc.be
Help | Terms & Conditions | Privacy Policy



bpost Security Notification

Dear Jane Smith,

We noticed a critical issue: **Password Expiry Notification**. To ensure your account remains secure, please follow the link below:

If you do not act within 24 hours, your account may be suspended.

Thank you for your immediate attention to this matter.

Sally Sneaky (IT Security Officer)
Email: support@bpost.be | Phone: +32 475 15 60 30
Visit our website: https://bpost.be

Help | Terms & Conditions | Privacy Policy

Gophish: The Training Ground

Gophish Platform

Goofish is a platform for conducting phishing simulations in a controlled environment.

Targeted Simulations

Simulations can be targeted to specific groups or individuals within a company.

Data Analysis

Goofish tracks user interactions, allowing for analysis of training effectiveness.

Flexibility and Control

Customization

The AI can be adapted to work with any company and tailored to specific departments or individuals.

Control

The cyber security team has control over the simulation parameters and can adjust them based on results.

The Human Element

1 AI

2 Cyber Security Team

3 Employees

The cyber security team plays a crucial role in understanding the AI, analyzing results, and adapting training programs.

The Future of Cyber Security Training

1

Advanced Simulations

AI-powered simulations will become more realistic, sophisticated, and challenging.

2

Continuous Learning

The cyber security team must stay ahead of the curve by continuously learning and adapting.

3

Ethical Use

AI must be used responsibly and ethically to ensure a safe and secure digital world.

Key Takeaways

1

AI is Powerful

AI can be a powerful tool for creating realistic phishing simulations.

2

Human Expertise is Crucial

The cyber security team must understand the AI and use it responsibly.

3

Continuous Learning is Essential

The cyber security landscape is constantly evolving, requiring ongoing learning and adaptation.

Next Steps

1

Explore AI Tools

Research and experiment with AI tools for cyber security training.

2

Develop Training Programs

Create targeted phishing simulations for specific departments or individuals.

3

Stay Informed

Keep up with the latest advancements in AI and cyber security.

Q&A

Please feel free to ask any questions you may have. I'm happy to discuss any details further.