SECURITY AWARENESS

Secure Your Workplace

Nume: Oscar Gal
Email: galoscar05@gmail.com

Content

01 Company (Rodeapps)

02 Why do we do Awareness?

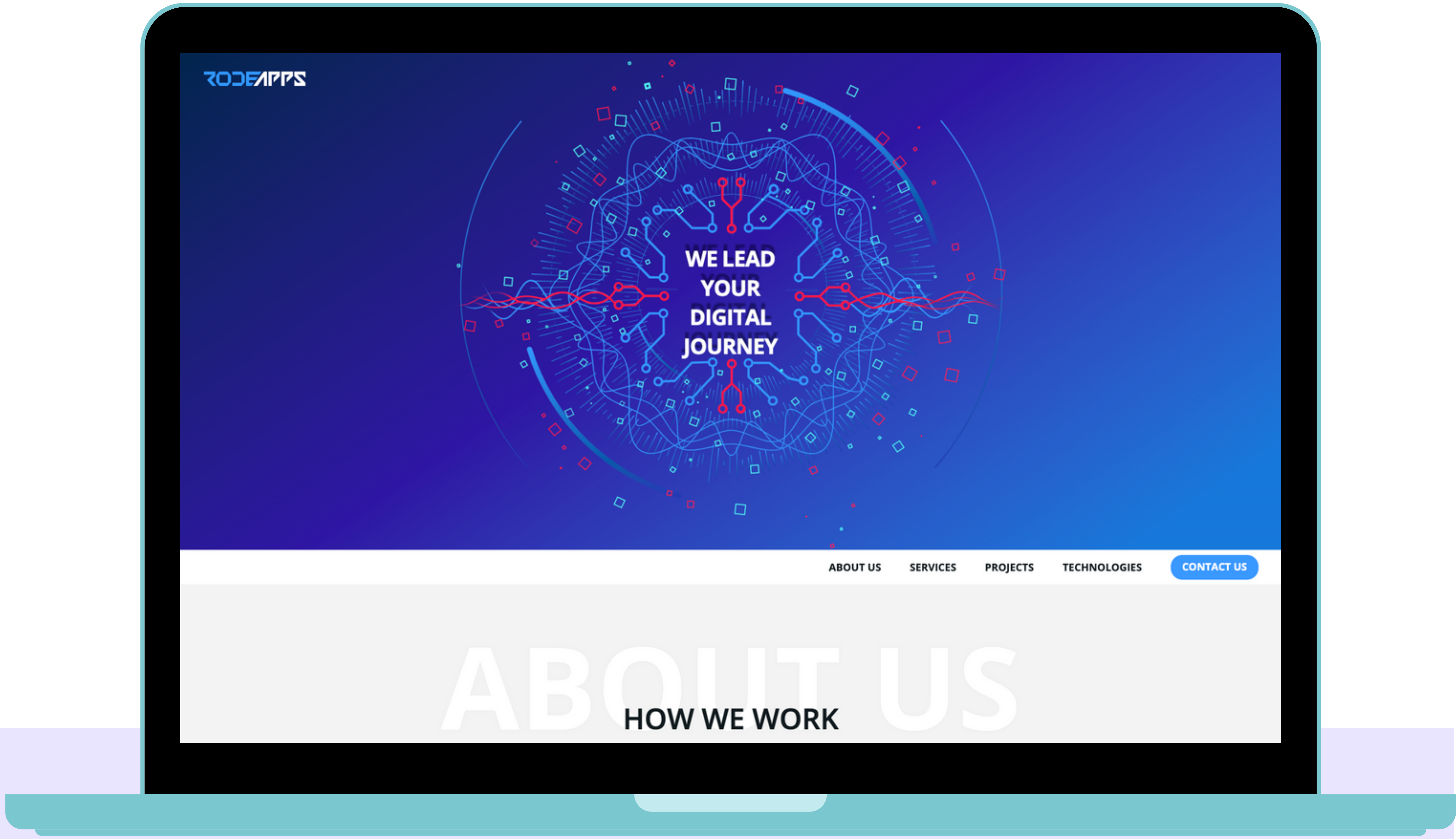
03 Security Awareness Themes

04 Social engineering

05 How to Identify Phishing and Social Engineering Attempts

06 Conclusion / Questions

Rodeapps



We are a team of technology enthusiasts that will lead your journey from a half-baked idea to a successful digital product.

As part of an innovation-centric agency, our professionals will understand your product idea, will analyze your business processes, and will find and implement a solution for all your technology needs.

Why do we do Awareness?

Security awareness is an essential aspect of protecting an organization from potential security threats, and it is important to keep employees informed and educated on the latest security practices to ensure the overall security of the organization.

01 Security awareness campaigns educate employees on basic security practices and common security threats, such as phishing scams and social engineering. This empowers employees to recognise and avoid potential security risks.

02 By raising employee awareness, organizations are better equipped to detect and prevent security breaches. For example, if employees are aware of the signs of a phishing scam, they are more likely to report suspicious emails and prevent a potential data breach.

03 Many industries are subject to strict regulations, such as HIPAA or PCI-DSS, that require organizations to implement security awareness programs.

04 Security awareness helps to protect sensitive information such as personal data, trade secrets, and financial information from falling into the wrong hands.

Security Awareness Themes I

Here are a few examples of common security awareness themes:

PHISHING AND SOCIAL ENGINEERING

This theme focuses on educating employees on how to recognise and avoid phishing scams and social engineering attacks, such as spear-phishing and whaling.

MOBILE DEVICE SECURITY

This theme focuses on the security risks associated with mobile devices, such as smartphones and tablets, and how to protect against them.

INTERNET SAFETY

This theme covers best practices for safe internet usage and ways to protect against online threats such as malware, viruses, and hacking

Security Awareness Themes II

PASSWORD SECURITY

This theme covers best practices for creating and managing strong passwords, and how to protect against password-related security threats.

PHYSICAL SECURITY

This theme covers best practices for protecting the physical security of an organisation, such as securing buildings and equipment.

CYBERSECURITY TRENDS AND THREATS

This theme covers the latest cybersecurity trends and threats, and how to protect against them.

Social engineering l

is a type of psychological manipulation used by cybercriminals to trick people into divulging sensitive information or performing actions that may compromise their security. It is a tactic that attackers use to exploit human psychology rather than technical vulnerabilities. Social engineering attacks rely on people's trust, naivety, and lack of knowledge about security to achieve their goals.thanks to technology.

PHISHING

This is a form of social engineering that involves tricking people into providing sensitive information, such as login credentials or financial information, through fake emails or websites.

PRETEXTING

This is a form of social engineering in which an attacker creates a fake identity and uses it to gain access to sensitive information or resources.

BAITING

This is a form of social engineering in which an attacker entices people to divulge sensitive information or perform actions by offering something of value in return, such as a prize or free service.

Social engineering II

SCAREWARE

This is a form of social engineering in which an attacker tricks people into purchasing software by showing fake security warnings or threats.

QUID PRO QUO

This is a form of social engineering in which an attacker offers assistance or information in exchange for sensitive information or access to resources.

These examples are not exhaustive and attackers come up with new tactics to deceive people. It's important for individuals to be aware of the various forms of social engineering, and to be skeptical of unsolicited requests for personal information, especially over the phone or email, and to be aware of the red flags that might indicate an attack.

How to Identify Phishing and Social Engineering Attempts I

STEP 1

Look for suspicious email addresses or URLs

Phishing emails often come from addresses that are similar to, but not exactly the same as, legitimate addresses. For example, an email from "support@paypa1.com" instead of "support@paypal.com". Also, be suspicious of links or URLs that contain spelling errors or that redirect to a different website than the one specified in the link.

STEP 2

Be wary of unsolicited requests for personal information

Legitimate organisations will not typically ask for personal information through email or phone. Be suspicious of any unsolicited requests for personal information, such as login credentials or financial information.

STEP 3

Be wary of urgent or threatening language

Phishing emails and social engineering attempts often use language that is designed to create a sense of urgency or fear. Be wary of emails or phone calls that use language such as "Your account will be closed unless you respond immediately" or "You must act now to avoid serious consequences."

How to Identify Phishing and Social Engineering Attempts I

STEP 4

Look for generic greetings and lack of personalization

Legitimate emails and phone calls will typically address you by name and may include other personal information. Be suspicious of emails or phone calls that use generic greetings such as "Dear customer" or "Hello".

STEP 5

Check for typos and poor grammar

Phishing emails and social engineering attempts are often poorly written and may contain typos and grammatical errors. Be suspicious of emails or phone calls that contain obvious errors.

STEP 6

Be skeptical of unsolicited requests for access

Legitimate organizations will not typically ask for remote access to your computer or network without a valid reason. Be suspicious of unsolicited requests for remote access, such as phone calls or emails that ask you to provide access to your computer or network.

It is important to note that these are just examples and attackers come up with new ways to deceive people every day, but being aware of these red flags can help you identify phishing and social engineering attempts and take appropriate action. It is also important to report any suspicious email or phone call to the appropriate department or IT team within your organisation.

Do you have any questions?

Send it to us! We hope you learned something new.