YOUR GUIDE TO EMAIL

SAFETY

!

Open?

Delete?

ZIRKLE TECH

CONTENTS

INTRODUCTION

Email plays a crucial role in communication in today's fast-paced digital world. It's an essential tool for both internal and external business communication. However, the convenience of email comes with a significant challenge — keeping your inbox safe from cyberthreats.

Email safety is like securing your virtual front door. It helps protect sensitive information, maintain data integrity and safeguard your digital reputation. Increasing cybersecurity concerns have made prioritizing email safety more critical than ever.

This eBook will serve as your first step to strengthening your inbox. Following the best practices outlined in this guide will give you insights into a more secure email experience.

Our goal is to empower you without overwhelming you, and to ensure that email becomes your source of success instead of burnout.

Let's dive in and discover how a few simple steps can amplify the security of your email communication.

THE IMPORTANCE

of email safety in protecting your digital life

Within your inbox lies a trove of sensitive data, from personally identifiable information to financial details. Inadequate protection could lead to unauthorized access, resulting in identity theft or fraudulent activities.

Spam emails serve as instruments for spreading phishing, malware and ransomware attacks. Prioritizing email security becomes imperative to thwart these insidious attacks.

Whether for business transactions or private conversations, maintaining the confidentiality of your emails is pivotal. Email safety assures that only intended recipients can access your messages.

> "Maintaining the confidentiality of your emails is pivotal".

Email account takeovers mirror unwelcome guests intruding on your privacy. They disrupt your peace by dispatching unsolicited emails, proliferating malware and causing chaos. Implementing safety measures erects barriers against these digital trespassers.

Complying with data protection laws isn't a choice; it's a mandate. Laxity can lead to legal entanglements and penalties. Prioritizing email safety serves as a road to legal compliance.

Imagine losing crucial emails due to accidental deletions or security breaches. Email safety measures function as a safety net, averting unfortunate incidents.

STEPS TO STAY SAFE FROM EMAIL TRAPS

Follow these simple steps to ensure the safety of your inbox:

✓ Secure your email account with a robust, unique password, as you would secure your front door. Make sure not to share it with anyone.

✓ Employ two-factor authentication (2FA) to add an additional layer of security. 2FA acts as a digital bodyguard by verifying your identity before granting access.

✓ Be cautious of suspicious email links and unfamiliar attachments. These could harbor digital trojans ready to take down your network.

✓ Exercise caution while sharing personal details. Reserve this for instances where the sender's identity is beyond doubt.

✓ Keep your email software and antivirus defenses updated to thwart security breaches.

✓ Avoid using public Wi-Fi for sensitive emails since data shared on open networks lacks the privacy you need.

✓ Stay vigilant against sophisticated phishing attempts capable of threatening your sensitive data.

✓ Regularly monitor your email for anomalies, ensuring prompt detection of any unusual activity.

✓ Safeguard crucial emails with secure backups, similar to how you safeguard your valuable items.

✓ Deploy spam filters to intercept sneaky attackers before they infiltrate your inbox.

✓ Use encrypted connections like HTTPS to shield data during transmission.

✓ Stay informed of emerging email threats to sustain a state of perpetual readiness.
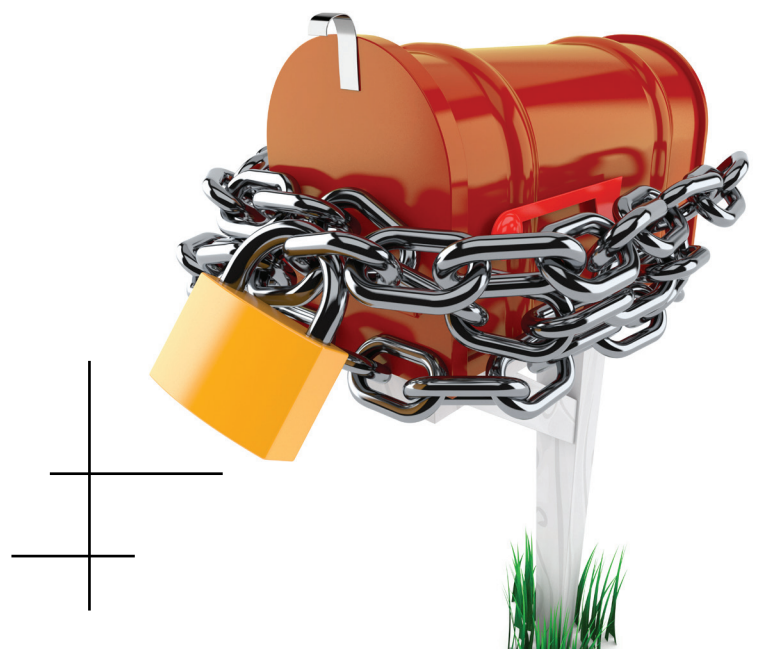
START YOUR EMAIL SAFETY JOURNEY NOW

Now that you've gained insights from this eBook, you can strengthen your email security like a pro.

It's important to remember that protecting digital conversations is your responsibility. By following the steps provided, you can take proactive measures to increase the security of your inbox and prevent potential risks.

If you need additional help improving your email security, our team is committed to supporting you on this journey.

Contact us to schedule a no-obligation consultation and let's start your email safety journey together.

sales@zirkletech.com
(440) 683-4921
www.zirkletech.com
www.zirkle-tech.com

🚩 SPOT THE RED FLAGS

Can you find the red flags in this email example?

Recognizing a BEC attack

Business Email Compromise (BEC) is a cyberattack where criminals impersonate trusted individuals or organizations through emails to deceive victims into transferring funds or sharing sensitive information.

To youremail@gmail.com

From joe@microsoft.security.com

Subject URGENT!! UPDATE ACCOUNT!!

Microsoft

Hello customer,

Your account infromation has been compromised.

Please update your account information immediately. For your account secruity upate password. We advise you to click the link below to update now.

microsoft/login.com

Thank you,

Microsoft Team

↩ Reply   ↪ Forward

WORD SCRAMBLE

Use the hints to unscramble the words.

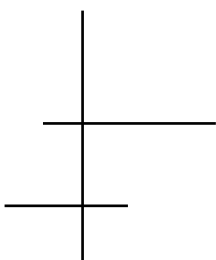### SOSUUPISCI LISNK

HINT: Avoid clicking these potentially harmful things in emails.

BIATLLSKC

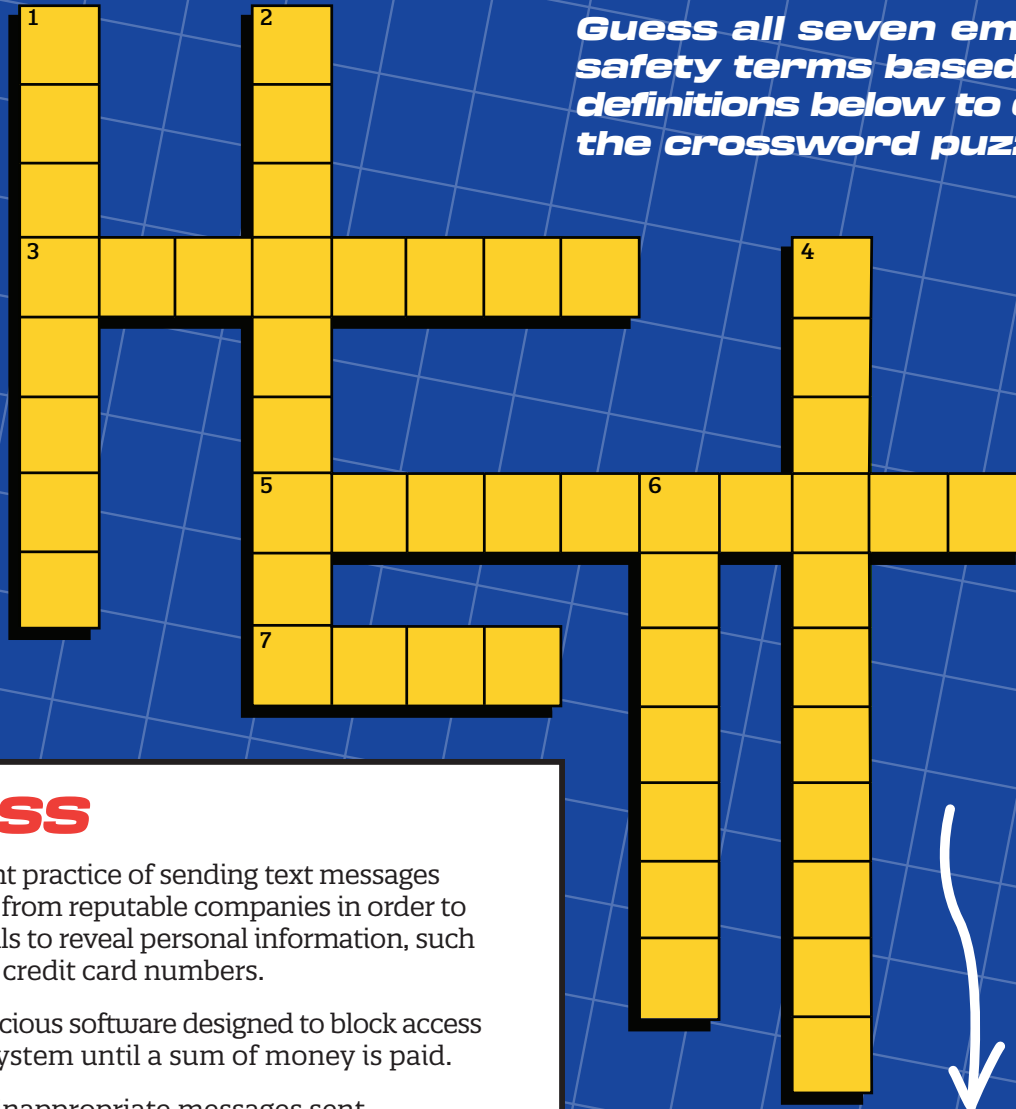**HINT:** Blocking emails from malicious domains

TYPNDCERE NOINECSONTC

HINT: Use these to access your email, such as HTTPS, to protect your data during transmission.

CROSSWORD

Guess all seven email safety terms based off the definitions below to complete the crossword puzzle!

ACROSS

3. The fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers.

5. A type of malicious software designed to block access to a computer system until a sum of money is paid.

7. Irrelevant or inappropriate messages sent on the internet to a large number of recipients.

DOWN

1. The fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

2. Never reuse or share these with anyone.

4. Be wary of unexpected or suspicious email _____.

6. Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

WORD SEARCH

```
E M X F Y O N U F E M B G W F
U R F I Q F P E R C O Z N H A
C C A W I H W A R T J W I A D
C V F W F S W Q N B V K S L W
N I T P L E P E F B J G I I A
V B X U R A T Y Q K O S T N R
M R G A M P M G W A A U R G E
P V C H W T N P U A A E E W V
P S F K O R L L R L R S V O V
N P M T L I M S H R I E L Z L
U B Q K Q H W U E A Z Z A A C
V F I J R H N J O J N M M U H
W O W G P E H Y S R X W D A D
S P O O F I N G L X J R P G F
G N I H S I H P E N O L C I S
```

ADWARE
BOTNET
CLONE PHISHING
MALWARE

SPOOFING
SPYWARE
WHALING
MALVERTISING
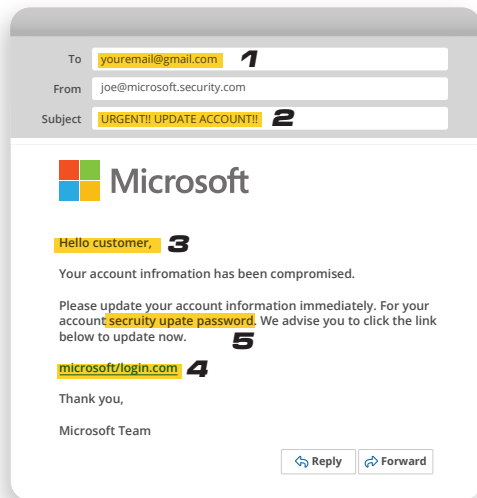**SCAREWARE**

ACTIVITIES KEY ✱✱✱

SPOT THE RED FLAGS

1. Non-official email address **2.** Urgent subject line
3. Unusual/improper greeting **4.** Unusual domain
5. Poor spelling and grammar

To: youremail@gmail.com **1**
From: joe@microsoft.security.com
Subject: URGENT!! UPDATE ACCOUNT!! **2**

■■ Microsoft

Hello customer, **3**

Your account infromation has been compromised.

Please update your account information immediately. For your account security upate password. We advise you to click the link below to update now. **5**

microsoft/login.com **4**

Thank you,

Microsoft Team

↩ Reply   ↪ Forward

WORD SCRAMBLE

SUSPICIOUS LINKS

BLACKLIST

ENCRYPTED CONNECTIONS

CROSSWORD

DOWN

1. Phishing
2. Passwords
4. Attachments
6. Malware

ACROSS

3. Smishing
5. Ransomware
7. Spam

WORD SEARCH

```
E M X F Y O N U F E M B G W F
U R F I Q F P E R C O Z N H A
C C A W I H W A R T J W I A D
C V F W F S W Q N B V K S I W
N I T P L E P E F B J G L N A
V B X U R A T Y Q K O S T G R
M R G A M P M G W A A U R G E
P V C H W T N P U A A E E W V
P S F K O R L L R L R S V O V
N P M T L I M S H R I E L Z L
U B Q K Q H W U E A Z Z A A C
V F I J R H N J O J N M M U H
W O W G P E H Y S R X W D A D
S P O O F I N G L X J R P G F
G N I H S I H P E N O L C I S
```