INFORMATION SECURITY

- Email Security
- Malicious Websites
- Good Information Security Practices

OPEN LEADERS | BY JELAGAT SHALEEN

Email Security

WHAT

Techniques for keeping sensitive information in email communication and accounts secure

WHY

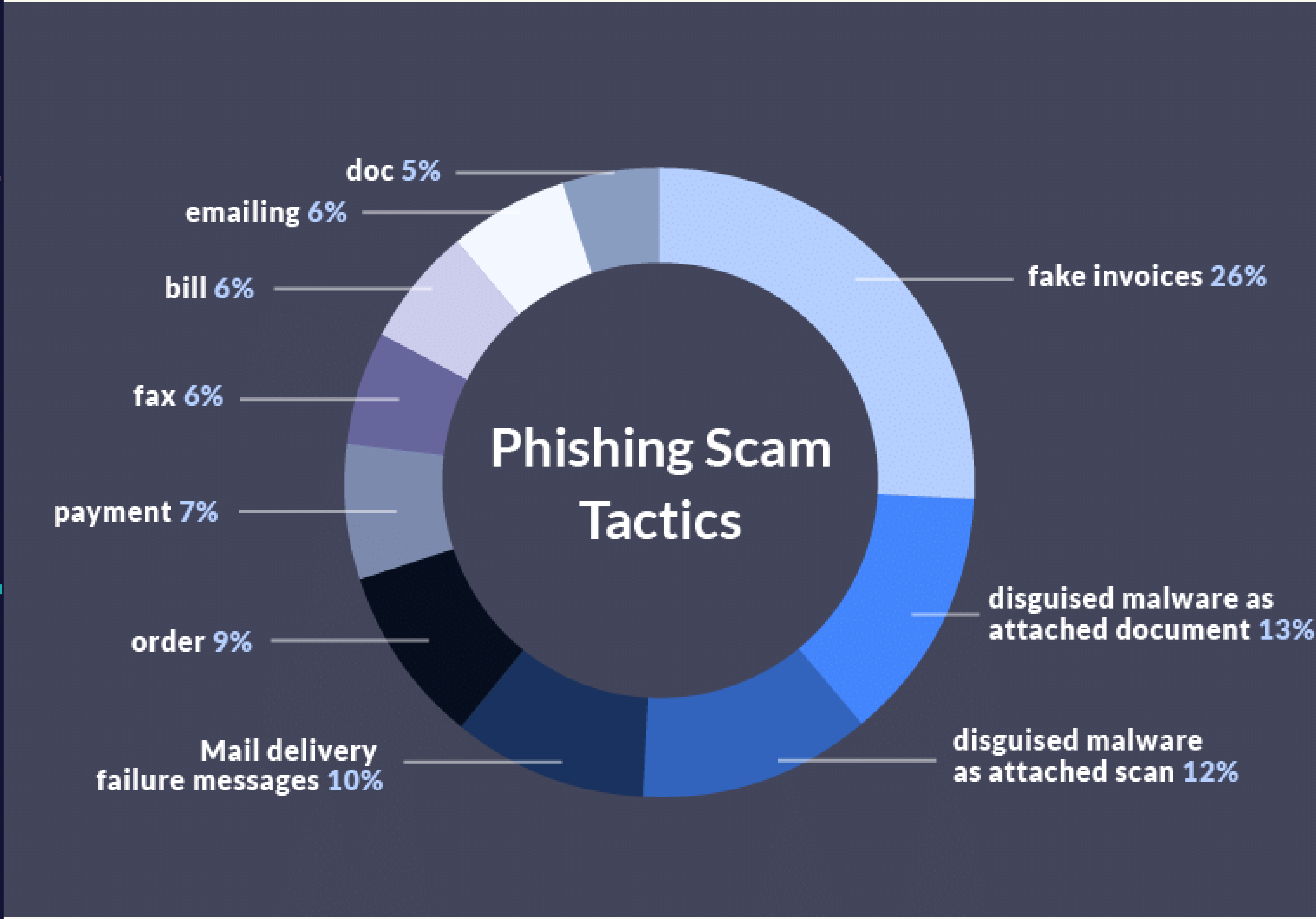
- Unauthorized access
- Loss
- Compromise

HOW

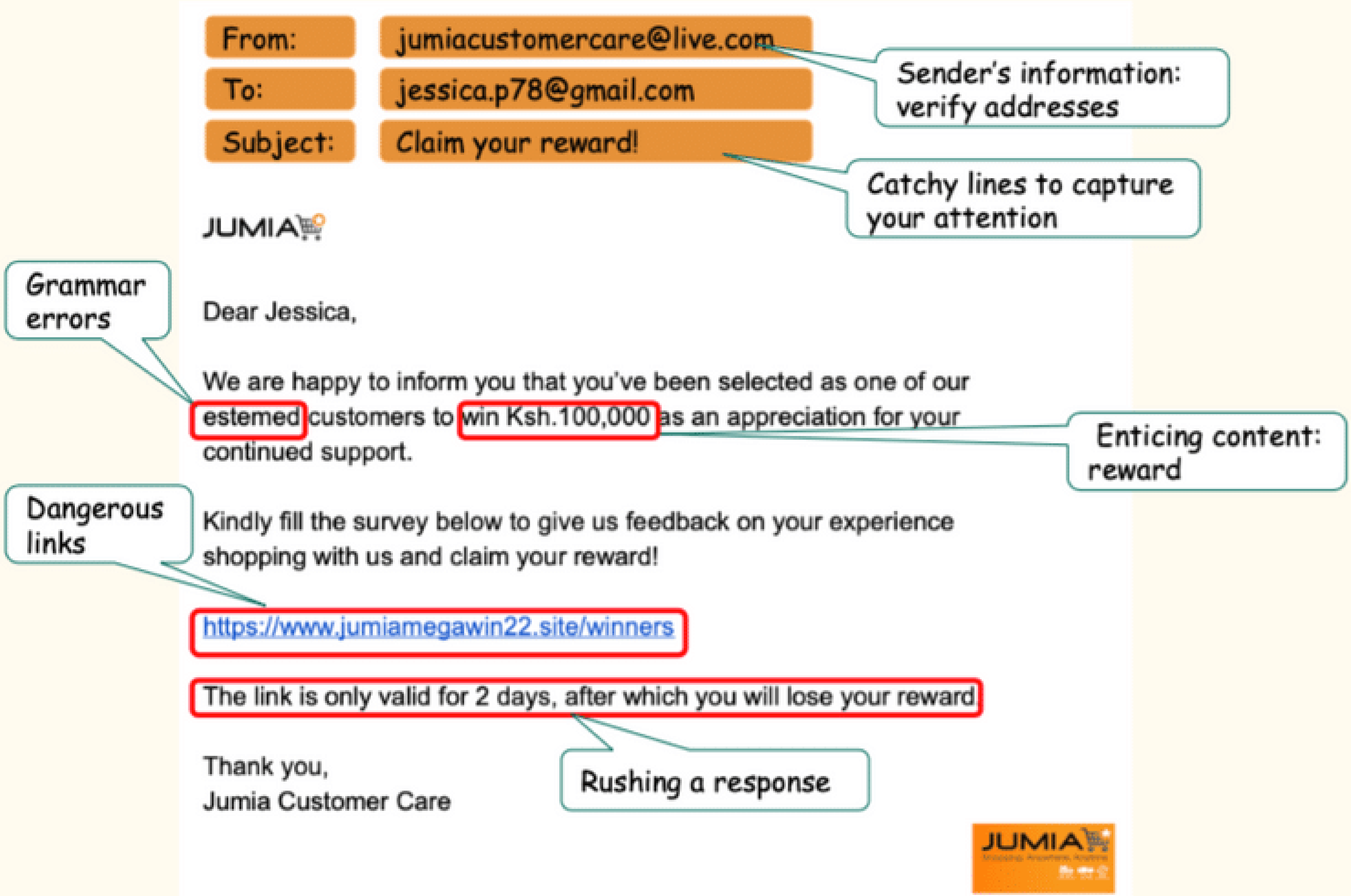
- Password Cycling
- Spam Filtering & Spyware Protection
- Secure Logins
- Email Encryption
- Employee Education

Categorizing phishing scams

45% OF ALL MAIL IS SPAM!



Mail Phishing



From: jumiacustomercare@live.com

To: jessica.p78@gmail.com

Subject: Claim your reward!

JUMIA

Dear Jessica,

We are happy to inform you that you've been selected as one of our estemed customers to win Ksh.100,000 as an appreciation for your continued support.

Kindly fill the survey below to give us feedback on your experience shopping with us and claim your reward!

https://www.jumiamegawin22.site/winners

The link is only valid for 2 days, after which you will lose your reward

Thank you,
Jumia Customer Care

Sender's information: verify addresses

Catchy lines to capture your attention

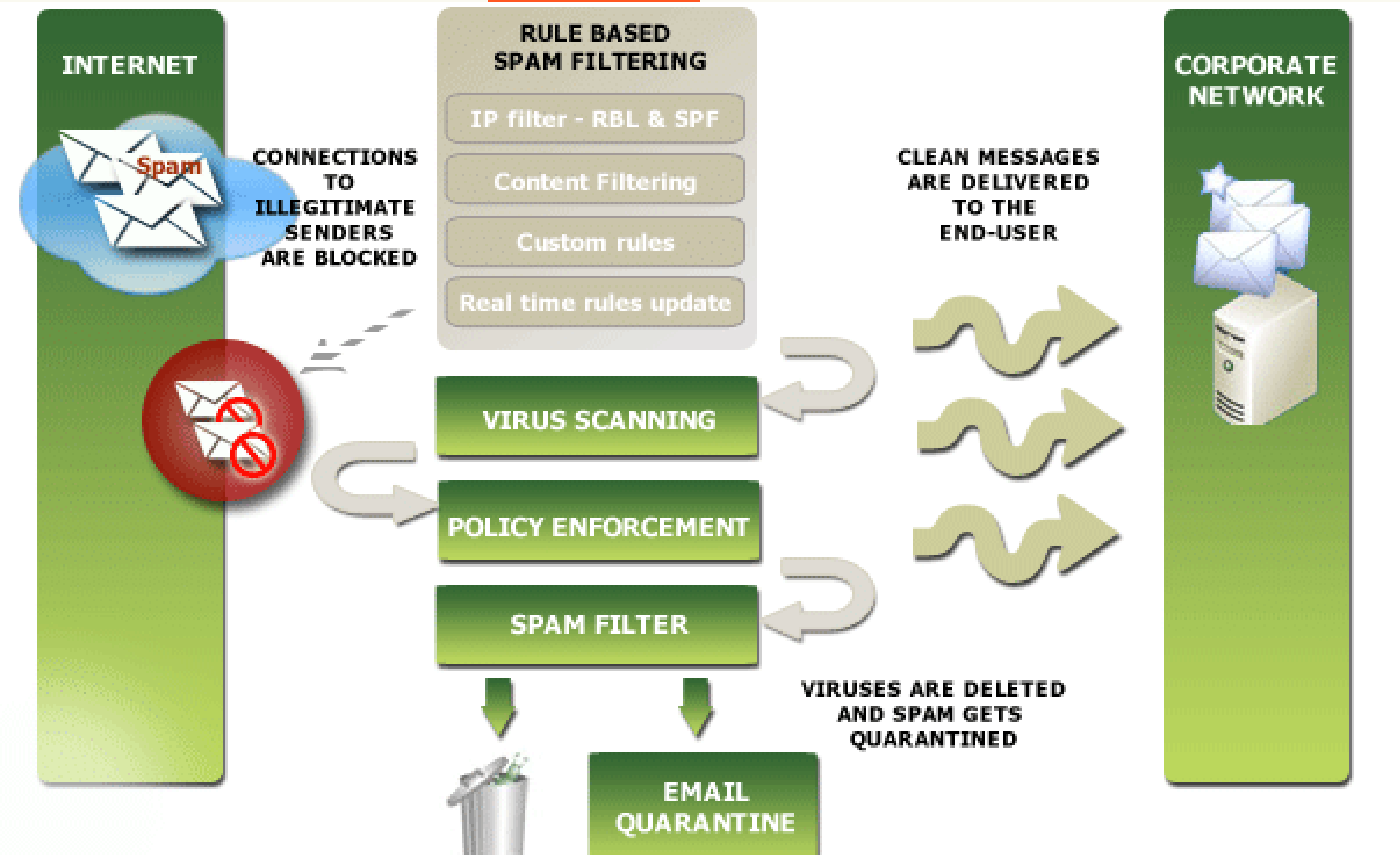
Grammar errors

Enticing content: reward

Dangerous links

Rushing a response

Mail Filtering


INTERNET
Spam
CONNECTIONS TO ILLEGITIMATE SENDERS ARE BLOCKED
RULE BASED SPAM FILTERING
IP filter - RBL & SPF
Content Filtering
Custom rules
Real time rules update
VIRUS SCANNING
POLICY ENFORCEMENT
SPAM FILTER
EMAIL QUARANTINE
VIRUSES ARE DELETED AND SPAM GETS QUARANTINED
CLEAN MESSAGES ARE DELIVERED TO THE END-USER
CORPORATE NETWORK

Malicious Websites

WHAT

- A site that attempts to install malware onto your device
- Look so legitimate

WHY

- Disrupt computer operation
- Gather personal information
- Gain total access to machine

HOW

- Malvertising: hijacked ads - download malicious software
- Drive-by downloads - Exploit kits
- Malicious Redirects
- Javascript Infections - download .js file
- URL Injection - embed malicious URLs

Protect Yourself from Malicious Websites

SOFTWARE UPDATE

Always keep software updated & Install patches as soon as possible.

SOFTWARE INSTALLATION

Never install any software you’re unfamiliar with or don't trust.

WEBSITE LINKS

Do some research to verify unfamiliar links before clicking.

INTERNET SECURITY SOFTWARE

Install security software that can identify malicious websites.

SENSITIVE INFORMATION

Protect your personal information and provide to only trusted personnel where necessary.

PROTECT YOUR SYSTEMS

Use of Firewalls, Strong passwords, Two-factor authentication, Security Policies

SAFE NETWORKS

Connect to networks you only trust and can verify them.
Avoid open, free networks - public WiFi

SECURITY TOOLS

Use of anti-virus, anti-spam, mail filtering and other detection tools

UP TO DATE SOFTWARE

Patch your software as soon as there's an update or an upgrade

DIGITAL FOOTPRINT

Be cautious of what you post online especially on social media platforms - location, personal details thank you