MINISTRY OF SECURITY

ALL ABOUT PHISHING

MINISTRY OF SECURITY

PHISHING?

Phishing attacks are social engineering attacks. Phishing is when an attacker sends a legitimate looking email "from" banks or any organization of that nature with faulty information to trick you into clicking on a link or opening an attachment to steal your information.

IT ONLY TAKES ONE CLICK!

HOW TO DETECT?

- Software based Detection–

1. Whitelist: This is similar to allowing entry who is having invitation card. Allow these only and other all are blocked.
2. Blacklist: Blacklisting makes it possible to block unwanted emails, lottery sms, inputs or traffic for a specified time.

- Visual Similarity–

Attackers create similar kinds of fake wave sites which look legitimate wave site but in reality, it is a fake wave site.

- Anomaly Detection–

Software detects abnormal behaviors in similar kinds of conditions where an increase of attacks get detected above the reference level using AI/ML.

USER TRAINING

Periodic training for the users should be provided and post training valuation of the training should also be evaluated through audit or feedback and number attacks reported.

MINISTRY OF SECURITY

TYPES

WHALING

Whaling is a highly targeted phishing attack – aimed at senior executives – masquerading as a legitimate email. This is also known as "executive phishing."

PREVENTION:

If you receive a suspicious email from a coworker, reach out to them directly to confirm its legitimacy.

MINISTRY OF SECURITY

SPEAR PHISHING

"Spear phishing" is a type of phishing campaign that targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents.

PREVENTION:

Users should always double-check the sender's email address before giving a response or responding to the mails.

MINISTRY OF SECURITY

PHARMING

Pharming is online fraud that involves the use of malicious code to direct victims to spoofed websites in an attempt to steal their credentials and data.

PREVENTION:

Avoid visiting unsecure "HTTP" websites.

MINISTRY OF SECURITY

DECEPTIVE PHISHING

This type of phishing uses deceptive technology such as email spoofing to send messages that appear to be from an address other than their own. Like other types of phishing emails, these messages may contain malicious links or attachments

PREVENTION:

Always use a good antivirus and also think twice before clicking links and attachments.

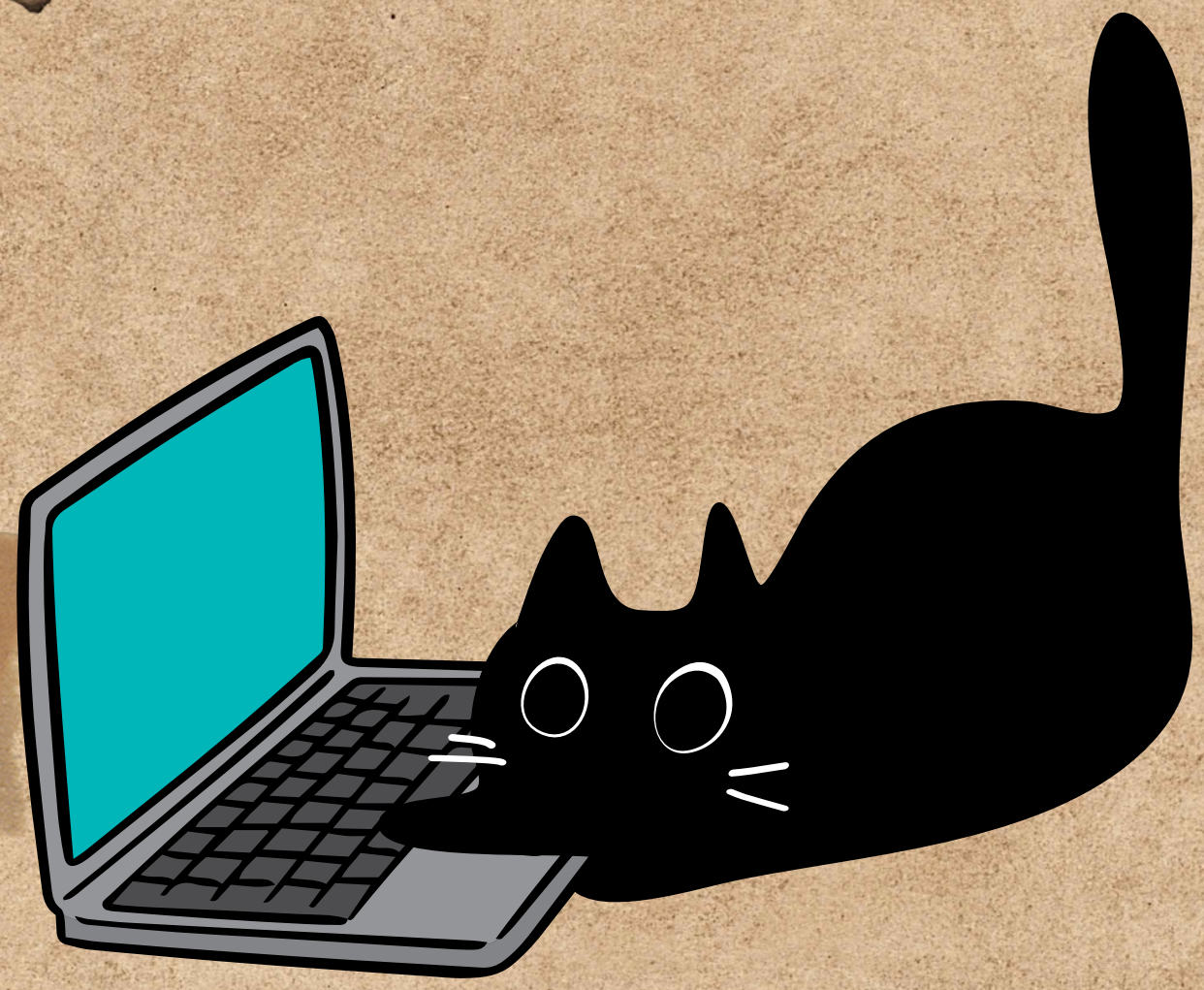
MINISTRY OF SECURITY

HTTPS PHISHING

HTTPS phishing is when a cybercriminal tricks you into giving up your personal information using a malicious website. To get you onto these sites, the phisher will hide the malicious link within an email, often masquerading as a link to a legitimate site.

PREVENTION:

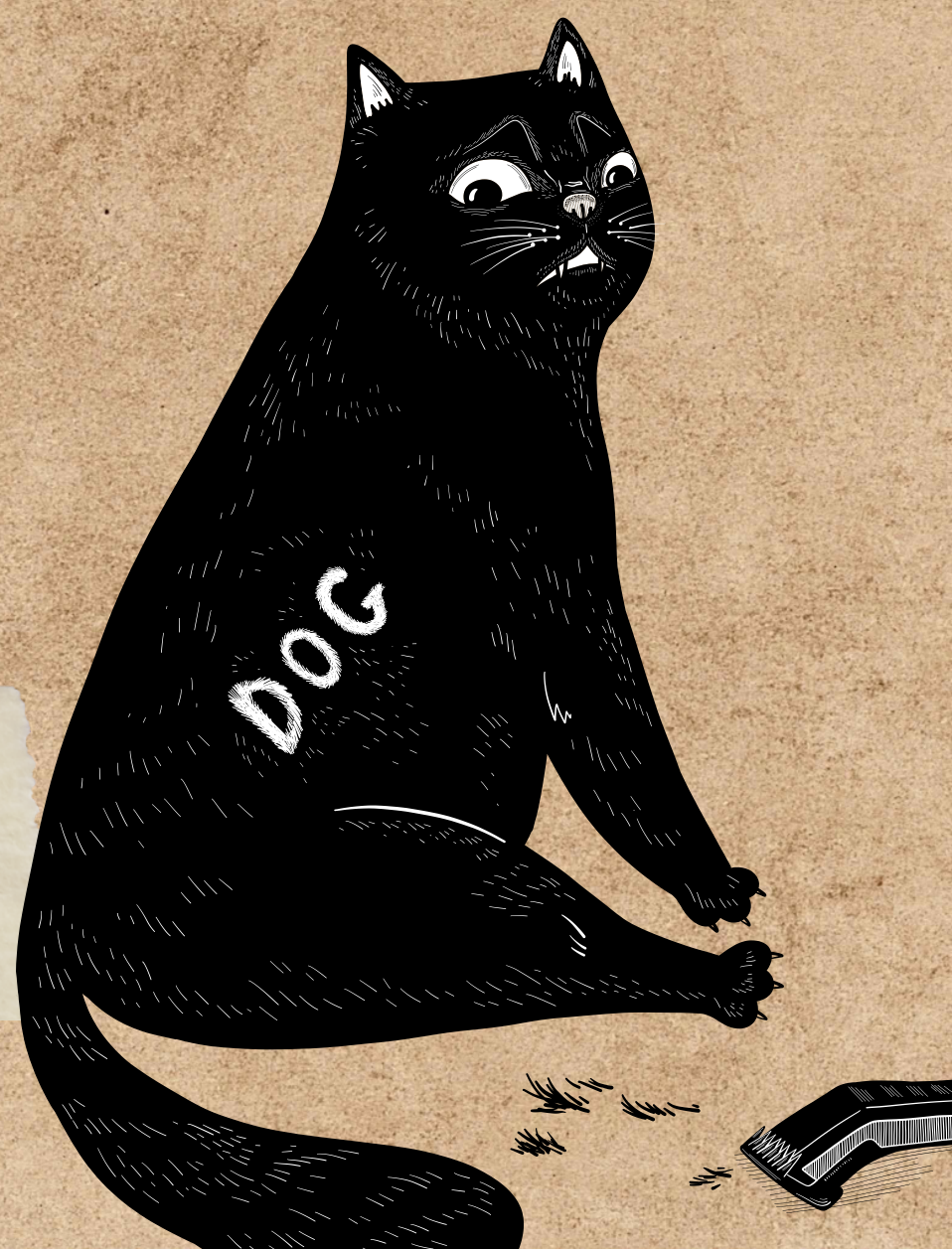
Always look closely at the URL of a site before logging in.



MINISTRY OF SECURITY

SOCIAL ENGINEERING

Social engineering is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information.



PREVENTION:

Avoid panicking and take your time to assess the legitimacy of the situation.

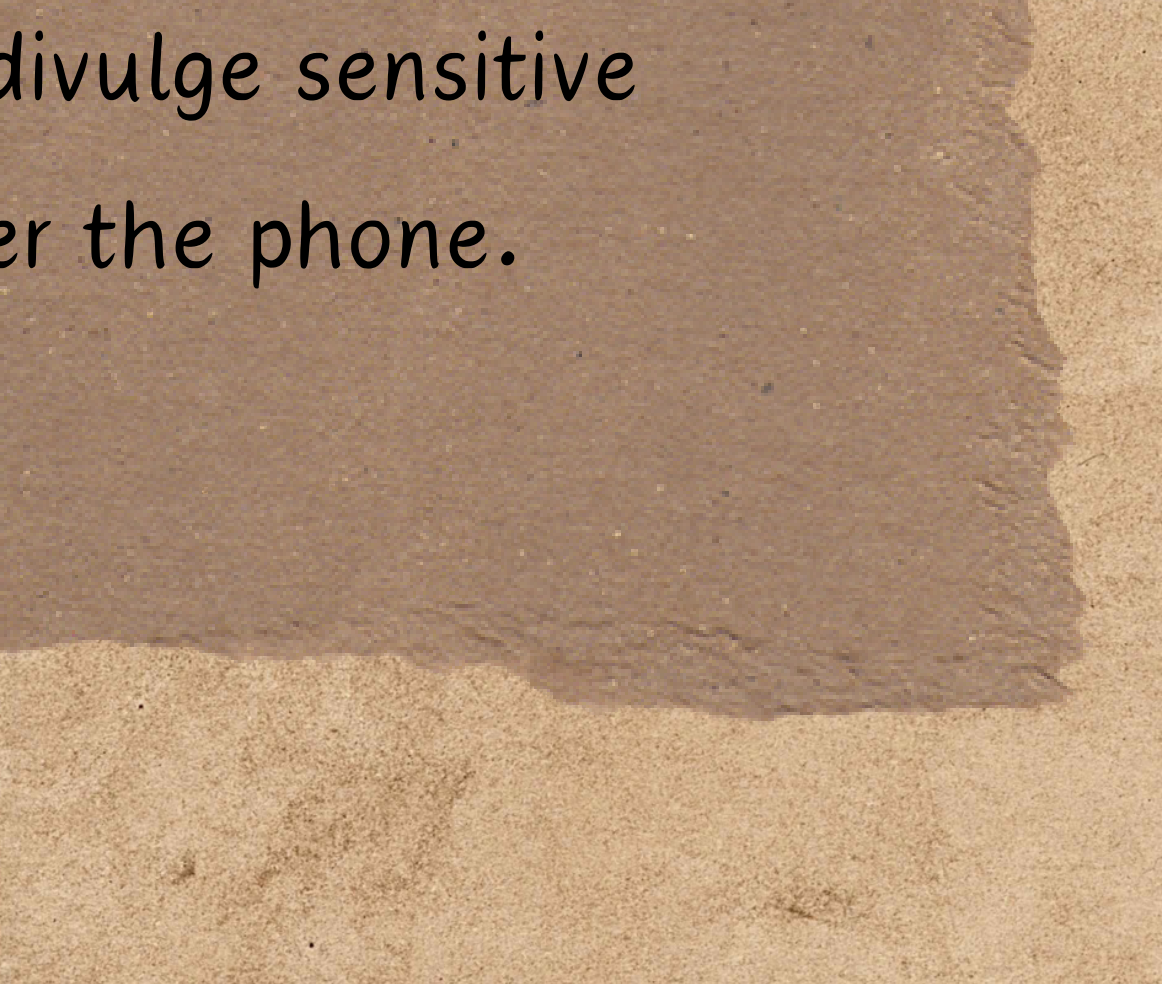
MINISTRY OF SECURITY

VISHING

Vishing is short for "voice phishing," which involves defrauding people over the phone, enticing them to divulge sensitive information over the phone.

PREVENTION:

Always use a good antivirus and also think twice before clicking links and attachments.



MINISTRY OF SECURITY

POP-UP PHISHING

Pop-up phishing is a type of attack that leverages adware and pop-up ads to trick users into downloading malware onto their devices

PREVENTION:

Enable a pop-up blocker and avoid clicking on any popup windows you encounter online.

MINISTRY OF SECURITY

SEARCH ENGINE PHISHING

Search engine phishing attacks attract users using fake product pages. The catch is that instead of being able to purchase the product, they're handing over their payment information to a scammer.

PREVENTION:

Avoid giving your payment information to websites other than trusted and reputable online vendors.

MINISTRY OF SECURITY

IMAGE PHISHING

Image phishing is an attack in which hackers disguise malicious code or different types of malwares using image files. Once you click on the image, your computer will begin downloading the malicious code stored within the image.

PREVENTION:

Never click on or download an image from a suspicious email message.

MINISTRY OF SECURITY

SMISHING

Smishing is the word that describes phishing over short message services (SMS). Phishing text messages usually use social engineering tactics and contain malicious links.

PREVENTION:

Avoid opening links from unknown phone numbers.

MINISTRY OF SECURITY

DOMAIN SPOOFING

Domain spoofing is a type of phishing attack in which the attacker impersonates a known person or company using a fake email domain.

PREVENTION:

Copy the sender's email address and compare it to the official email address listed on the company's site.

MINISTRY OF SECURITY

MAN IN THE MIDDLE

A man-in-the-middle (MITM) attack is an attack in which a hacker steals your information by getting in between you and a trusted party.

PREVENTION:

Always use a VPN when connecting to public Wi-Fi networks.

POINTERS ON HOW TO PREVENT

KEEP THINGS UP TO DATE

USE 2 FACTOR OR MFA

ESSENTIAL ENDPOINT SECURITY

PHISHING SIMULATION

MINISTRY OF SECURITY

FOLLOW US FOR MORE FREE CHECKLISTS | PLAYBOOKS TEMPLATES | VIDEOS

PLAYBOOK MADE WITH ❤ MINISTRY OF SECURITY

SECURITY & PRIVACY MADE EASY