Cyber Flyer For Your Knowledge

Traditional cyber awareness programmes are failing to keep people safe online

cybsafe.com

DON'T GET **HOOKED**

How to Recognize and Avoid **PHISHING ATTACKS**

What is Phishing?

The Go-To Social Engineering Strategy

Phishing attacks are **techniques** used by cybercriminals to con users/employees into **revealing sensitive information** or **installing malware** by way of electronic communication.

Phishing Attack Methods

MOST COMMON TYPE OF PHISHING ATTACK
HIGHLY TARGETED TYPE OF PHISHING ATTACK
THE MOBY DICK OF PHISHING ATTACKS

MASS-SCALE **PHISHING**

Attack where fraudsters **cast a wide net of attacks** that aren't highly targeted

SPEAR **PHISHING**

Tailored **to a specific victim or group of victims** using personal details

WHALING

Specialized type of spear phishing that **targets a "big" victim** within a company

e.g., CEO, CFO, or other executive

HOOK, LINE & SINKER

The tricks hackers use to try to get your personal information and how to avoid it.

Common Phishing Tactics

Phishing happens when you get an email from what looks like a trusted source (such as Northwestern or your bank) asking for personal information.

Messages are often urgent or threatening

You may be asked to click a link or open an attachment to verify information

Graphics, URLs, and signatures often look legitimate

What to Do if You Suspect Phishing

The "phishing" lure may look convincing, but don't take the bait

Don't open attachments or click email links unless you know they are legitimate

Check for odd sender email addresses or misspellings

Search for the real website online and confirm its address

Do not reply or send passwords or other personal information

Not sure? Forward a copy of the email to security@northwestern.edu

Delete messages you confirm to be phishing attempts from your inbox

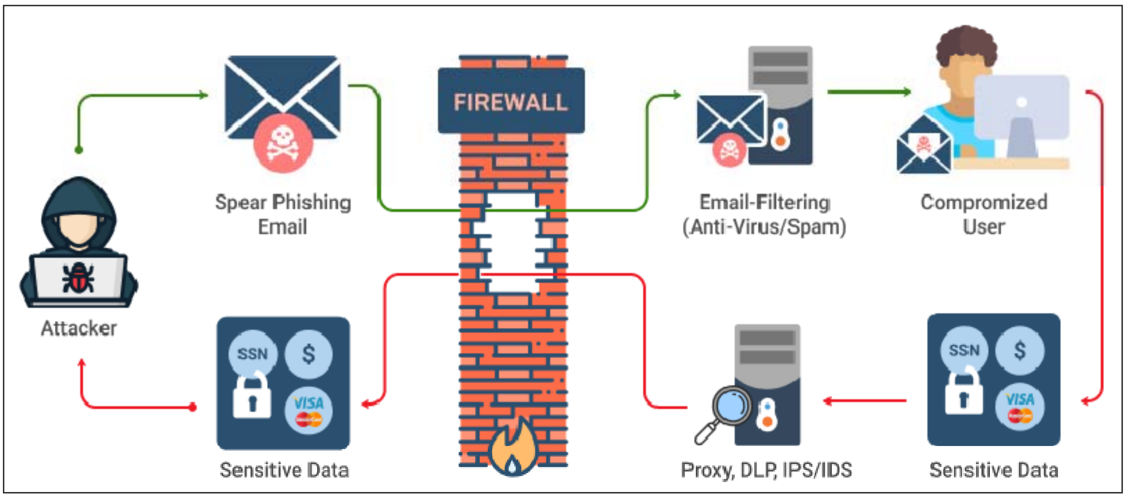
Uh-Oh, did you get hooked?

If you think you may have clicked something suspicious, let us know—we're here to help: **security@northwestern.edu**

Northwestern | INFORMATION TECHNOLOGY www.it.northwestern.edu

Top Cyber Threats

9 Cyber Threats that are guaranteed to ruin your day



HOW TO DEAL WITH PHISHING EMAILS

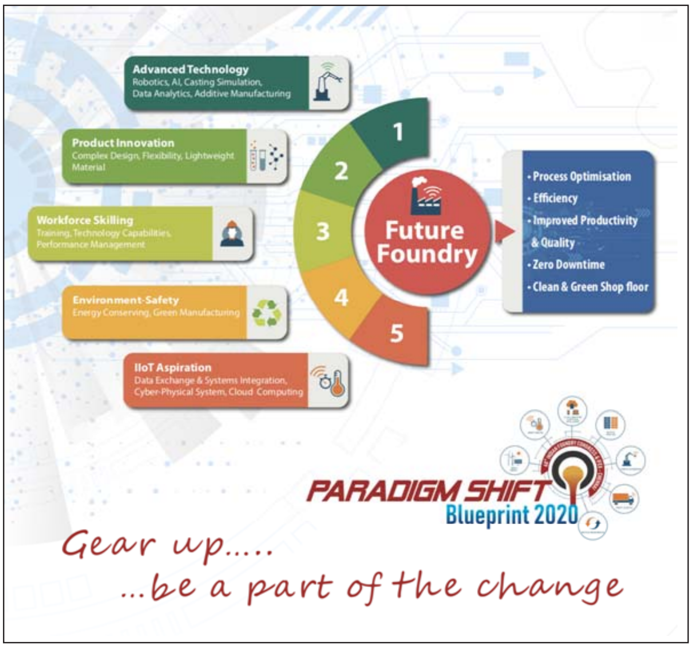
DO NOT RESPOND IN ANY WAY AND DO NOT OPEN ANY LINKS, ATTACHMENTS OR WEBSITES.

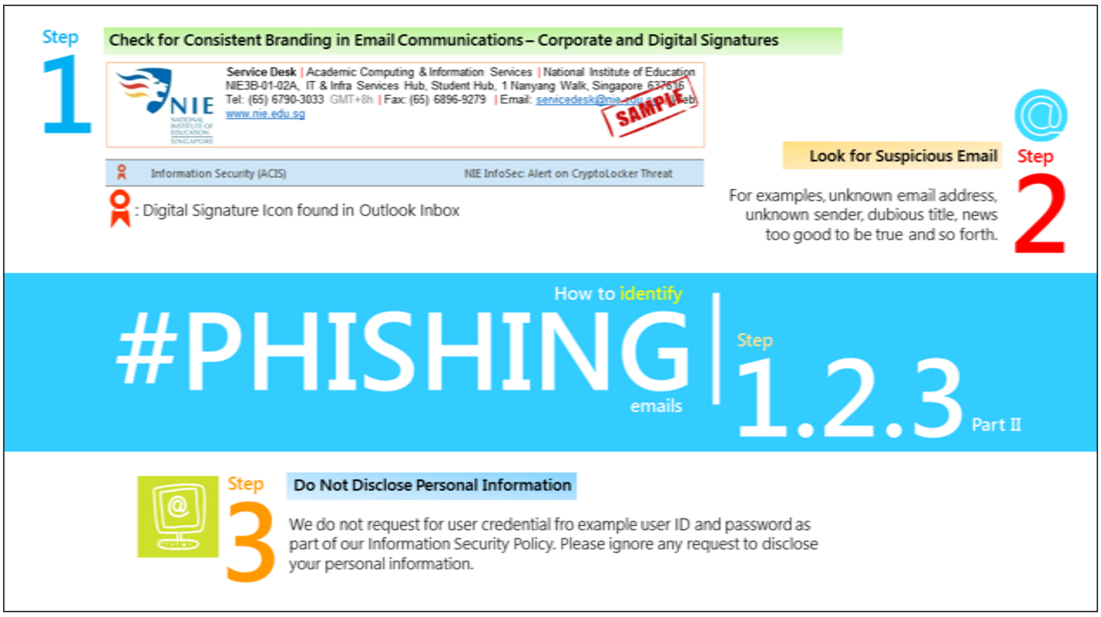
CONTACT THE COMPANY USING A KNOWN, OFFICIAL METHOD TO VERIFY THAT THE COMMUNICATION IS FRAUDULENT.

REVIEW BANKING AND CREDIT CARD STATEMENTS. CONTACT CUSTOMER SERVICE IF SUSPICIOUS ACTIVITY IS FOUND.

IMMEDIATELY CHANGE THE PASSWORD OF ALL ONLINE LOGINS.

INSTALL OR UPDATE THE ANTIVIRUS AND MALWARE SCANNERS ON YOUR COMPUTER.


Advanced Technology
Robotics, AI, Casting Simulation, Data Analytics, Additive Manufacturing
Product Innovation
Complex Design, Flexibility, Lightweight Material
Workforce Skilling
Training, Technology Capabilities, Performance Management
Environment-Safety
Energy Conserving, Green Manufacturing
IIoT Aspiration
Data Exchange & Systems Integration, Cyber-Physical System, Cloud Computing
1
2
3
4
5
Future Foundry
• Process Optimisation
• Efficiency
• Improved Productivity & Quality
• Zero Downtime
• Clean & Green Shop floor
PARADIGM SHIFT
Blueprint 2020
Gear up.....
...be a part of the change



Step 1 Check for Consistent Branding in Email Communications – Corporate and Digital Signatures

Service Desk | Academic Computing & Information Services | National Institute of Education
NIE3B-01-02A, IT & Infra Services Hub, Student Hub, 1 Nanyang Walk, Singapore 637616
Tel: (65) 6790-3033 GMT+8h | Fax: (65) 6896-9279 | Email: servicedesk@nie.edu.sg | Web:
www.nie.edu.sg

SAMPLE

Information Security (ACIS) NIE InfoSec: Alert on CryptoLocker Threat

: Digital Signature Icon found in Outlook Inbox

Look for Suspicious Email Step 2

For examples, unknown email address, unknown sender, dubious title, news too good to be true and so forth.

How to identify #PHISHING emails | Step 1.2.3 Part II

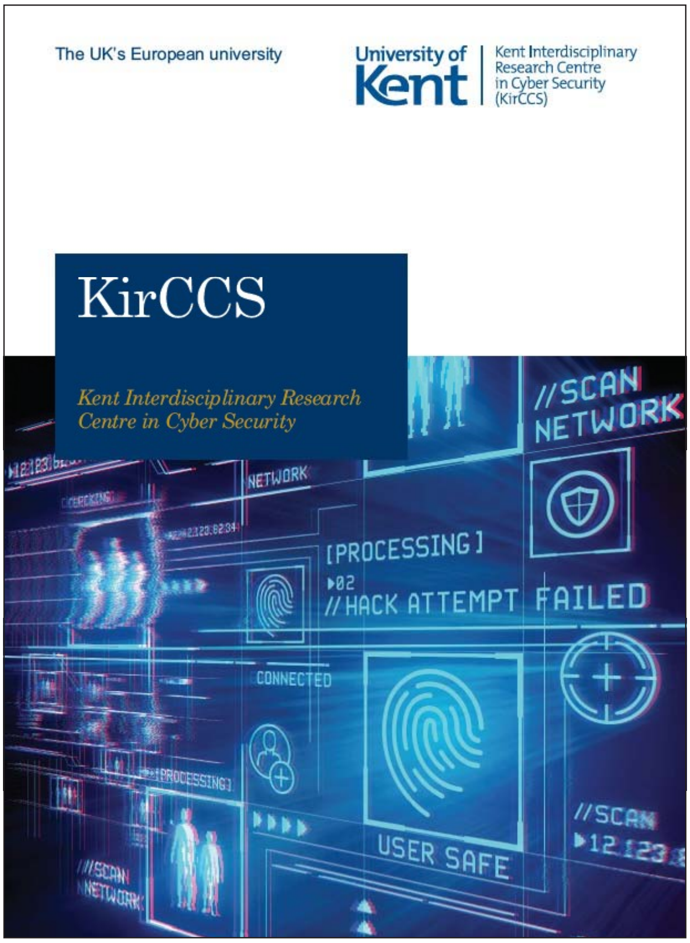
Step 3 Do Not Disclose Personal Information

We do not request for user credential fro example user ID and password as part of our Information Security Policy. Please ignore any request to disclose your personal information.

The Hidden Costs of Cybersecurity Detection Really Adds-Up

When you invest in detection-based security tools, you budget for the known costs, such as purchase price and licensing fees.

Our research uncovers the surging hidden costs of reactive, detection-based security.

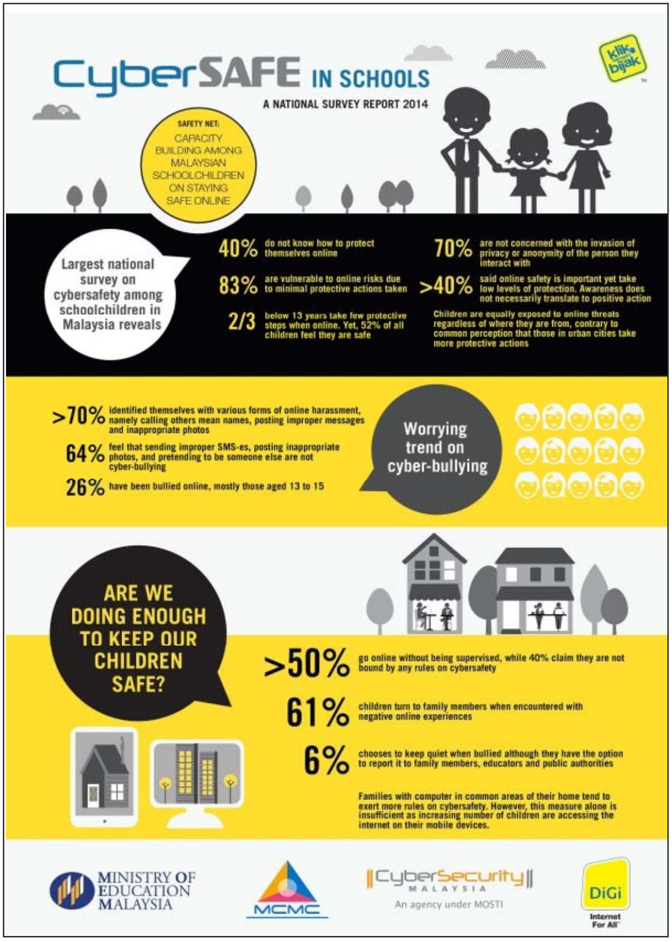


The UK's European university

University of Kent | Kent Interdisciplinary Research Centre in Cyber Security (KirCCS)

KirCCS

Kent Interdisciplinary Research Centre in Cyber Security



CyberSAFE IN SCHOOLS

A NATIONAL SURVEY REPORT 2014

SAFETY NET: CAPACITY BUILDING AMONG MALAYSIAN SCHOOLCHILDREN ON STAYING SAFE ONLINE

Largest national survey on cybersafety among schoolchildren in Malaysia reveals

40% do not know how to protect themselves online

83% are vulnerable to online risks due to minimal protective actions taken

2/3 below 13 years take few protective steps when online. Yet, 52% of all children feel they are safe

70% are not concerned with the invasion of privacy or anonymity of the person they interact with

>40% said online safety is important yet take low levels of protection. Awareness does not necessarily translate to positive action

Children are equally exposed to online threats regardless of where they are from, contrary to common perception that those in urban cities take more protective actions

Worrying trend on cyber-bullying

>70% identified themselves with various forms of online harassment, namely calling others mean names, posting improper messages and inappropriate photos

64% feel that sending improper SMS-es, posting inappropriate photos, and pretending to be someone else are not cyber-bullying

26% have been bullied online, mostly those aged 13 to 15

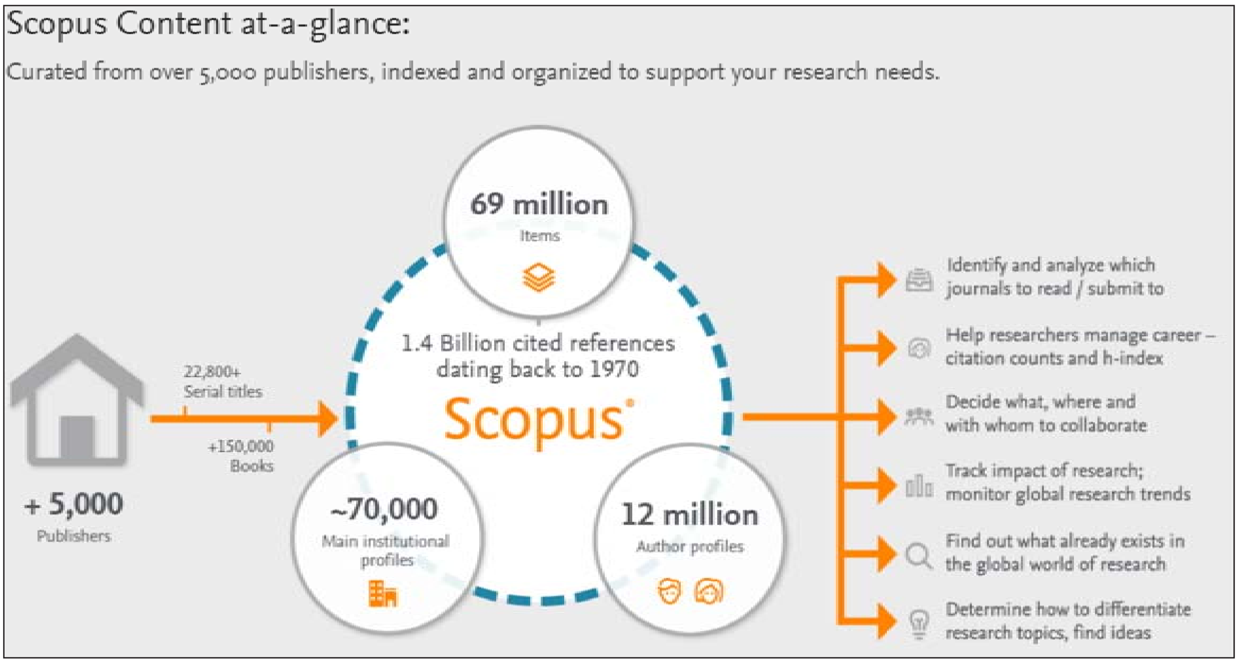
ARE WE DOING ENOUGH TO KEEP OUR CHILDREN SAFE?

>50% go online without being supervised, while 40% claim they are not bound by any rules on cybersafety

61% children turn to family members when encountered with negative online experiences

6% chooses to keep quiet when bullied although they have the option to report it to family members, educators and public authorities

Families with computer in common areas of their home tend to exert more rules on cybersafety. However, this measure alone is insufficient as increasing number of children are accessing the internet on their mobile devices.



Scopus Content at-a-glance:

Curated from over 5,000 publishers, indexed and organized to support your research needs.

+ 5,000 Publishers

22,800+ Serial titles

+150,000 Books

69 million Items

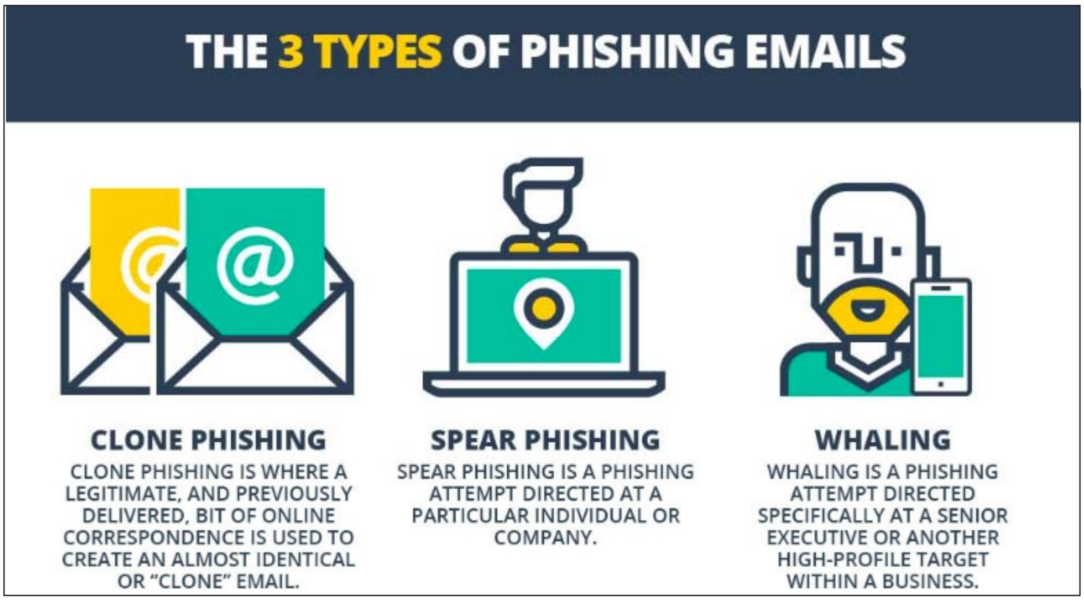
1.4 Billion cited references dating back to 1970

Scopus®

~70,000 Main institutional profiles

12 million Author profiles

- Identify and analyze which journals to read / submit to
- Help researchers manage career – citation counts and h-index
- Decide what, where and with whom to collaborate
- Track impact of research; monitor global research trends
- Find out what already exists in the global world of research
- Determine how to differentiate research topics, find ideas



THE 3 TYPES OF PHISHING EMAILS

CLONE PHISHING

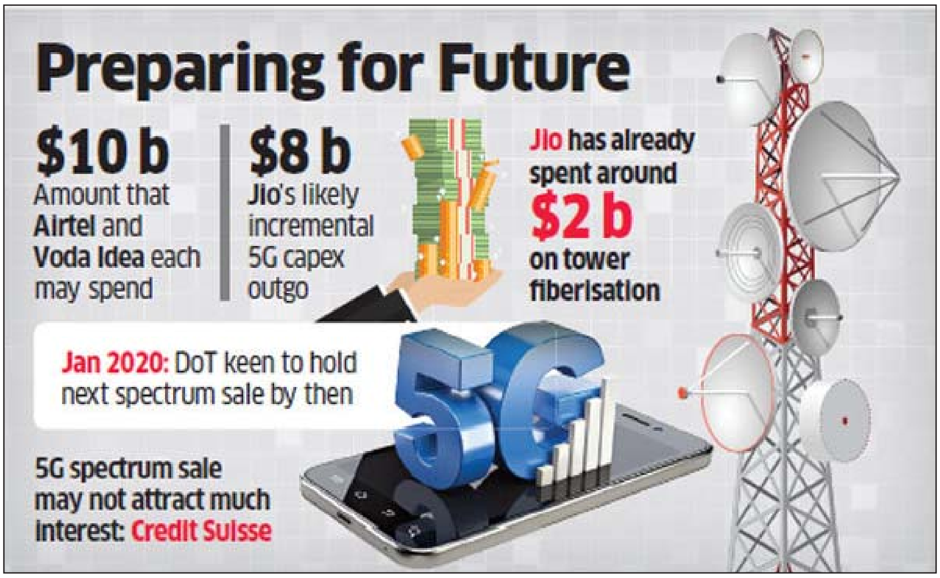
CLONE PHISHING IS WHERE A LEGITIMATE, AND PREVIOUSLY DELIVERED, BIT OF ONLINE CORRESPONDENCE IS USED TO CREATE AN ALMOST IDENTICAL OR "CLONE" EMAIL.

SPEAR PHISHING

SPEAR PHISHING IS A PHISHING ATTEMPT DIRECTED AT A PARTICULAR INDIVIDUAL OR COMPANY.

WHALING

WHALING IS A PHISHING ATTEMPT DIRECTED SPECIFICALLY AT A SENIOR EXECUTIVE OR ANOTHER HIGH-PROFILE TARGET WITHIN A BUSINESS.



Preparing for Future

$10 b Amount that Airtel and Voda Idea each may spend

$8 b Jio's likely incremental 5G capex outgo

Jio has already spent around $2 b on tower fiberisation

Jan 2020: DoT keen to hold next spectrum sale by then

5G spectrum sale may not attract much interest: Credit Suisse