THE ASSISTING INDIVIDUAL DEFENCE™ SERIES: EMAIL

WHAT IS THIS ?

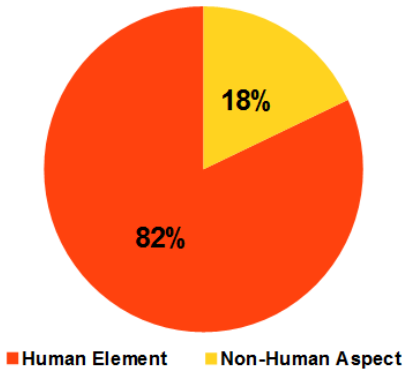
Assisting **I**ndividual **D**efence (**AID**) is an **upskilling training** series aimed at non-IT persons working in non-IT areas, e.g. Education, Finance, HR, Legal, Management, Manufacturing, Marketing, Medical, Procurement, Sales, etc. It aims to impart targeted specific skills to increase the cybersecurity defensive posture of an organization by **spreading the burden of defending against specific types of attacks across the entire organization headcount**.

In particular, **AID:Email** (AIDE™) aims to enable any non-technical staff to be able to self-identify **any** attack email that gets past technical defences by using our proprietary approach and tool, and how to react appropriately to it **without needing to involve IT**. This helps reduce the likelihood of bad guys **phish**ing, **ransomware**-ing, **malware**-ing or **data-exfiltrating** your company via targeting your employees who do in-office / remote work email or who use home computers for business.

WHY BOTHER WITH ANTI-PHISHING & ANTI-RANSOMWARE TRAINING?

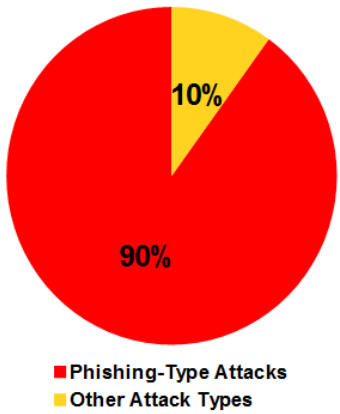
1. Bad guys targeting your company will go after any employee they can. Why lower their success rate by targeting the technical IT department when they can go after Management, HR, Finance, etc, instead? Here are some statistics :

% of Total Reported Security Breaches involved :



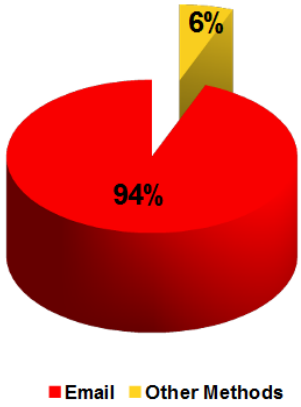
Source : Verizon 2022 Data Breach Investigations Report

% of Total Data Breaches are caused by :



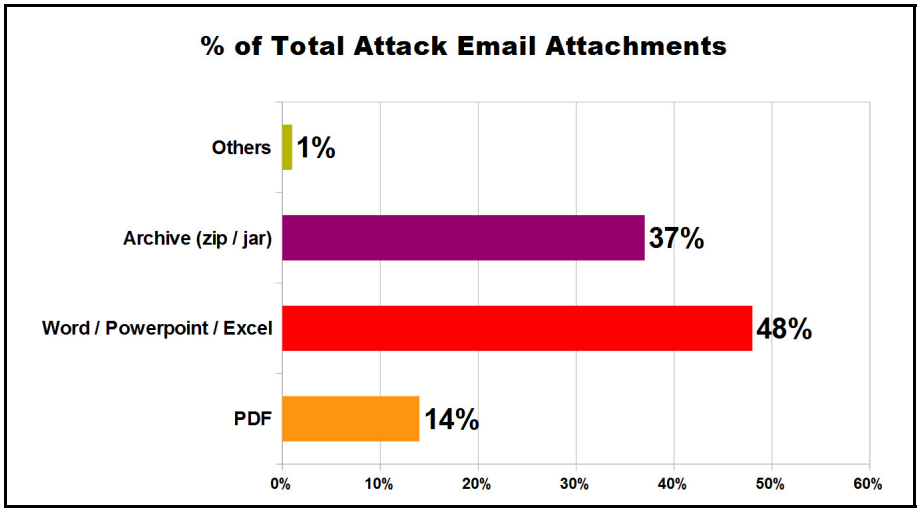
Source : Cisco 2021 Cybersecurity Threat Trends Report

% of Malware is delivered by



Source : Verizon 2021 Data Breach Investigations Report

% of Total Attack Email Attachments



Source : Cisco 2018 Annual Cybersecurity Report

ThinkSECURE™
Security Starts Here

www.securitystartshere.org

2. The unrelenting and increasing rate of attacks combined with staff shortages and legal compliance burdens has also made many cybersecurity staff get burn-out : a **2022 survey showed 54% OF THEM WANT TO QUIT CYBERSECURITY COMPLETELY (https://www.techrepublic.com/article/54-of-security-professionals-currently-want-to-quit-their-jobs)**.

3. The constant stream of attacks is only going to increase over time, with corresponding ever-increasing work stress on your IT and Cybersecurity teams. How do you cope if your IT / Cybersecurity people start resigning and you can't find replacements or if any new hires you find demand more pay for less experience?

4. Bad guys are constantly increasing the sophistication of their spear-phishing attacks; General security-awareness training isn't effective or is counter-productive (e.g. people end up not daring to open attachments and how then do you get work done?); People get over-reliant on imperfect technology (e.g. real legitimate emails wrongly end up inside junk-mail folders while spear-phishing emails can still end up inside inboxes).

HOW DOES AIDE™ ANTI-PHISHING & ANTI-RANSOMWARE TRAINING HELP YOU?

Wouldn't it be helpful for you if...
...**EVERY ONE** of your people...
...could learn...
...how to spot and avoid...
...**ANY** attack email...
...**WITHOUT** needing help from IT?

With the **ASSISTING INDIVIDUAL DEFENCE™ : EMAIL** (**AIDE™**) training, they can, and help spread out the defence load!

1. **UPSKILL EVERY EMPLOYEE TO BECOME PART OF YOUR DEFENCE!**
It doesn't matter if they are in Finance, HR, Legal, Management, Manufacturing, Medical, Procurement, Sales, Teaching, etc, or if they work for a commercial, educational or a non-profit organization - every employee **CAN BE ABLE TO HELP DEFEND YOUR ORGANIZATION**!

2. 3-hour-long practical training enables non-technical users to become technical-level extension of your Cybersecurity and IT team defences;

3. Enlist your non-technical department staff in the fight against ransomware and other threats by equipping them with the technical ability to more easily identify an attack email that makes it past your technical defences!

4. Reduce amount of incidents and helpdesk-escalation rates!
By giving your non-technical people the ability to be a first-line of defence against the bad guys without involving IT, this will lighten the burden of your IT and Cybersecurity teams in dealing with constant attacks against your organization and mitigate burnout;

5. And if your employees bring work home, how do you ensure that their own home environment isn't any less protected from attackers targeting them with email-laden malware and ransomware? AIDE™ allows you to extend your defence into the homes of your employees, making their home computers more resistant to email attack vectors.

THE ASSISTING INDIVIDUAL DEFENCE™ SERIES: EMAIL

HOW IS AIDE™ BETTER THAN END-USER SECURITY-AWARENESS TRAINING?

Many vendor-delivered end-user-level training and security awareness sessions are generic and focused on simply telling you "don't do this" or "don't do that", but don't teach you ***EXACTLY HOW*** to avoid sophisticated threats. End-user security-awareness training also often does not factor in continued inventiveness and creativity of attackers in bypassing automated defences. Those therefore do not impart sufficient technical-level depth to make a substantial difference at the front lines.

A simple question : After going through all the prior end-user training and security-awareness programmes, do **ALL** your non-technical end-users now possess **ACTIONABLE TECHNICAL-LEVEL SKILLS** that allows them to self-confirm that an email is malicious **WITHOUT NEEDING TO ESCALATE TO YOUR IT TEAM** ?

In comparison, our very-targeted, very-focused and cost-effective **AIDE™ UPSKILLING TRAINING** converts **TECHNICAL-LEVEL** cybersecurity skills into easy-to-apply everyday practical steps that **ANYONE** can apply to validate whether any email that makes it past your technical anti-spam/anti-phish hardware/software and arrives inside their mailbox is legitimate or not, **WITHOUT NEEDING TO ESCALATE TO YOUR IT TEAM**.

ALL your non-technical end-users can now become a technical-level extension of your Cybersecurity / IT-team and the last line of real defence against phishing and ransomware-laden emails that make it past your outer automated defences!

Why focus specifically and exclusively on email? As per the preceding graphics charts, email is the single largest delivery mechanism for targeting an organization through its end-users. So it makes sense to go after the biggest threat first.

Using our proprietary methodology and tool, we will teach your non-technical end-users how to easily spot different types of creative approaches that attackers take when sending spear-phishing and other social-engineering-attack emails to your mailboxes. The session includes a **practical exercise segment so that attendees can practice what is taught**, along with **access to our proprietary online tool** that complements the AIDE™ training session.

BENEFITS

- Enable your **NON-TECHNICAL** end-users to be self-checking on **EVERY** email inside their work and home mailbox;
- **Lighten your IT / Cybersecurity team workload** by reducing number of "report phishing email" reports they receive and frees them to focus on more value-added tasks;
- **Show that you are trying to reduce corporate risk** caused by the Great Resignation and ever-increasing governance and compliance demands stemming from PDPA, GDPA, etc;
- Hospitals, Healthcare, Schools, Law Firms, Banks, Insurance Companies, etc - **reduce** probability of phishing, ransomware and other incidents arising from end-user email interaction from **disrupting your mission-critical systems**;
- **Reduce your corporate third-party liability and public-relations nightmare** by lowering employees' vulnerability to ransomware and other malware delivered via spear-phishing emails;
- **Removes end-user excuses** that "I didn't know it was a malicious email" or "I am not trained to spot fake emails"; Now the only remaining reason an end-user can give is "I can't be bothered to check" and thus **make your Consequences Policy so much easier to apply**;

THE ASSISTING INDIVIDUAL DEFENCE™ SERIES: EMAIL

- **Applicable to ALL email software** and can even be applied for your own personal / home email if you work, study or conduct business from home to **prevent infection via work-from-home environments**!

WHO IS IT MEANT FOR?

- HR department employees;
- Finance department employees;
- Procurement department employees;
- Marketing department employees;
- Sales department employees;
- Senior, Mid and Supervisory Management;
- School Teachers / Students;
- Lawyers;
- Doctors / Nurses;
- Administrative staff;
- and **EVERY NON-TECHNICAL PERSON WHO USES EMAIL IN A WORKPLACE, SCHOOL, HOSPITAL AND HOME**

HOW LONG IS THE SESSION?

Up to 3 hours, depending on the degree of attendee interaction during the practical exercise segment.

Ideally, paid sessions are intended to be run on-site at your organization's premises for maximum effect. However, so long as attendees can access their work and/or personal email inboxes during the session using their laptops, the session can be run at any physical location subject to minimum session size and space constraints.

Contact us today for pricing and availability in your country; Please kindly email from your company email address and provide your company name as this training is intended for organizations with non-technical employees.