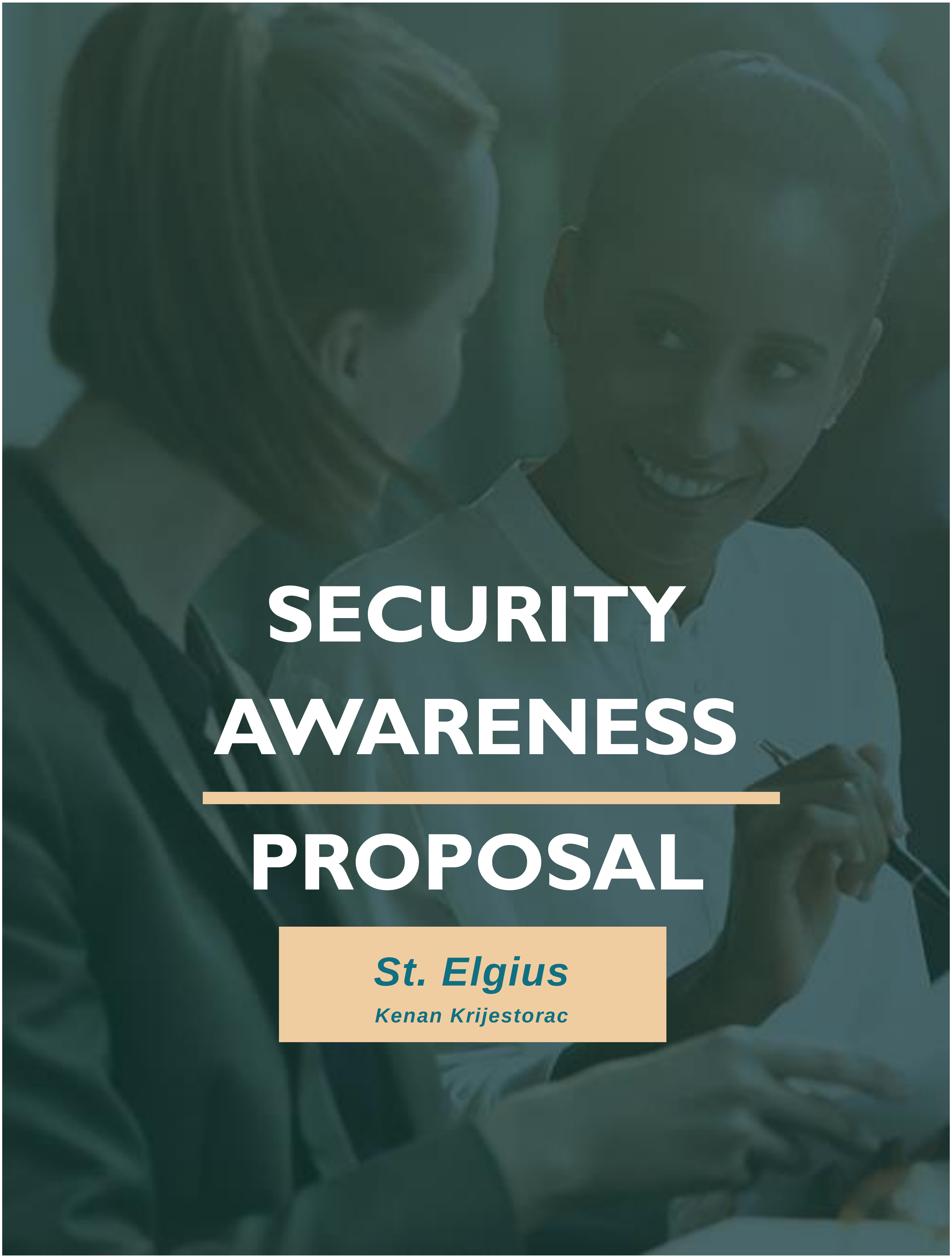


SECURITY AWARENESS

PROPOSAL

St. Elgius

Kenan Krijestorac

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Security awareness is an ever-growing key aspect of business. Daily announcements are made about a new data breach, vulnerability, or related issue. The majority of these attacks are launched against businesses such St. Elgius. Human error is becoming a common component in the security incidents that enterprises face.

The ***purpose*** of the *Security Awareness Proposal* presented in this document is to mitigate several common pitfalls that end users succumb to and the practices that they fail to adhere to, which consequently result in a financial loss and breach in privacy for our organization.

Since St. Elgius is a non-profit, medium-sized healthcare organization, it is critical to minimize the amount of unnecessary spending as a result of poor security awareness training. Awareness training will save our organization a plentiful amount of money in the long run and will ensure customer satisfaction and trust. The *Security Awareness Proposal* will focus on the two primary cybersecurity threats: phishing/email security and password strength/security.

This proposal will address important topics for implementing a successful security and awareness training program:

- **Intended Audience / Scope of the Plan:** In this section, the proper audience is outlined so that it is known which employees, contractors, etc. will be responsible for participating in the plan. Additionally, the details of the plan will be discussed in greater detail.

- **Assessment of Potential Weaknesses:** This section provides justifications for the need of implementing a Security Awareness Proposal within our organization.

- **Implementation Plan / Timelines:** This section provides which activities will be carried out, and the times and dates for specific security and awareness training modules.

- **Methods / Plan Measurement:** This section describes the tools and methods that will be used to deliver training to current staff and new hires. Additionally, a measurement will be provided to track the deployment of the plan over our various locations and employees.

- **Project Charter:** This section will provide a summary of the full project plan.

- **Training Aids:** This section provides customized visual aids for St. Elgius to reinforce proper security awareness.

- **Maintenance:** This section describes the plan for ongoing maintenance and updated training.

2. INTENDED AUDIENCE / SCOPE OF THE PLAN

Intended Audience

The proposal of implementing the *Security Awareness Proposal* was developed for C-level executives, so that they are able to determine the path to pursue for deploying a security awareness plan for the organization.

The intended audience for the *Security Awareness Proposal* includes all personnel within our healthcare organization. The program will require our approximate 15,000 employees that are spread across four hospitals, three outpatient surgery centers, twenty physician offices, and five mobile offices to engage in the program.

Scope of the Plan

The scope of the *Security Awareness Proposal* covers key topics that will aid in the mitigation of falling prey to standard phishing tactics and password vulnerabilities. The plan will be focused on increasing awareness on phishing/e-mail security and password strength/security. The scope includes awareness and training that users will have to undergo as well as the essential information associated with the success of the plan, such as assessment of weaknesses, implementation, measurement, maintenance. It is the intent of the plan to provide end users with the skills and awareness necessary to better protect St. Elgius' information as well as their personal information. These actions include, but are not limited to: proper password creation, reporting any suspicious emails, and following rules established to succumbing to phishing attacks.

3. ASSESSMENT OF POTENTIAL WEAKNESSES

According to a study conducted by IBM, human error is the main cause of 95% of cyber security breaches (Verizon). The implementation of a proper security and awareness training and/or campaign is an integral element in mitigating attacks on our organization.

Failure to implement a plan is the first step in which we fail our patients, clients, stakeholders, etc. We potentially put millions of people at risk of dealing with unnecessary litigation fees, recovery fees, and so on.

Phishing / Email Security

Without proper awareness and training on the various methods of phishing attacks that adversaries utilize, leaves the organization's assets potentially weak to attack. A study conducted by Verizon determined that 94% of malware is delivered via email and that 32% of breaches involve phishing (Verizon). Our employees are more likely to fall victim to these common phishing attacks:

- **Business Email Compromise (BEC):** Adversary spoofs an email address to solicit information from various departments for financial gain. For example, to acquire a wire transfer from the finance department, or gain sensitive documents from the human resources department.
- **Domain Spoofing:** An adversary changes the email domain to resemble that the email is coming from an official domain within the organization.
- **Spear Phishing:** An adversary utilizes social engineering to target specific individuals within the organization in order to deceive them into downloading or visiting a malicious attachment.

Password Strength/Security

Password strength and security also play a critical role in fortifying our organization from adversaries. Weak, default, and stolen passwords attribute to 63% of confirmed data breaches (Verizon). Many end users recycle passwords for more than one account. Consequently, using the same password for multiple accounts can result in several of those accounts being compromised. Easy-to-guess passwords increase the likelihood of an

4. IMPLEMENTATION PLAN / TIMELINE

	Jan.	Feb.	Mar.	Apr.	May	Jun.	Jul.	Aug.	Sept.	Oct.	Nov.	Dec.
Change end user, system, and network passwords.	■			■			■			■		
Conduct a simulated phishing exercise.		■	■	■				■	■	■		
Computer-based training for phishing attacks – Key identifiers: grammar/spelling, urgency, suspicious links, email header		■						■				
Computer-based training for password strength and security – Importance, common passwords, do's and don'ts			■						■			
Brown Bag Seminar – Reviews basics of phishing and password strength and security		■			■			■			■	

Table 1

CONT. IMPLEMENTATION PLAN / TIMELINE

A visual representation for the implementation plan for the training exercises and modules is displayed in Table 1 (pg. 6).

The implementation of the plan will take a centralized program communication model, where the CIO and/or the IT security program manager will communicate with the organizational unit management. The unit management will be responsible for having respective personnel complete the awareness and training offerings within the times in which they are offered.

The *Security Awareness Proposal* is structured in order to avoid repetitive and strenuous training on the personnel. The implementation of the plan is strategically laid out to maximize productivity and allow our employees to be able to retain the information.

- **Password Resets:** End users, system, and network passwords will be reset every 90 days in order to strengthen passwords, and ideally prevent adversaries from retaining access within our accounts.
- **Phishing Simulation:** Simulated phishing attacks will be carried out over two three-month spans. The simulated attack will be deployed to various departments over the course of the three-month span.
- **Phishing Computer-based Training:** The CB phishing training will be administered bi-annually. These trainings are offered at the beginning of each phishing simulation in order to test the retention and awareness of the personnel. The second training will ask participants to offer feedback.
- **Password Computer-based Training:** The CB password training is administered bi-annually. The training is offered the month before two of the password resets so that users are more likely to recall the training that they had recently undergone. The second training will ask participants to offer feedback.
- **Brown Bag Seminars:** The seminars are offered on a quarterly basis where personnel will learn review the fundamentals of phishing tactics and password strength and security. Employees will be required to at least one seminar over the course of the year.

Additionally, visual aids depicting key identifiers for phishing attacks and strong password recommendations/techniques will be distributed across the organization in various locations. Posters, flyers, etc. will be deployed within employee breakrooms, workspaces, cafeterias, bulletin boards, and other similar locations to emphasize the importance of the program.

5. METHODS / PLAN MEASUREMENT

Tools and Methods

- **Current Staff:** Training will be administered based on the implementation plan displayed in Table 1. End users will be able to access the computer-based training through the organization's web portal. Phishing and password strength and security training will be required on a bi-annual basis. The first phishing training will be available through the entire month of February and the second will be available August. The first password strength and security training will be available throughout the entire month of March and the second will be available in September. Brown bag seminars will be available a to-be-determined date in the months of February, May, August, and November.
  - Computer-based training on phishing will take approximately 30 minutes to complete, and computer-based training on passwords will take approximately 15-20 minutes.
  - Brown bag seminars will last approximately 30 minutes, followed by a question and answer. However, employees are only required to attend one seminar for the entire year.
- **New Hires:** Training for those who are in the process of becoming employees will be required to complete both computer-based training for phishing attacks and passwords concurrently. Those hired within the first half of the year will be also be required to complete the training within the second half of the year. Those hired within the second half of the year will only be required to complete the one training on phishing and passwords. New hires will still be required to attend one brown bag seminar.

Plan Measurement

Each of the trainings will measured and scored independently of one another. The participation of employees in the computer-based training and brown bag seminars will be recorded.

Phishing Simulation: The employees that fall victim to the phishing simulation will be recorded and tested in more versatile manners. The contents of responses to the simulated malicious emails will be stored, reviewed, and discussed with the end user to reinforce the importance of properly identifying phishing emails (Measurement). Additionally, annual markers for each individual phishing launch will be measured within the first half and second half of the year to determine if the average scores of the simulation were lower than the previous. The number of reports of the simulated email will also be used as a measurement.

6. CONT. PLAN MEASUREMENT

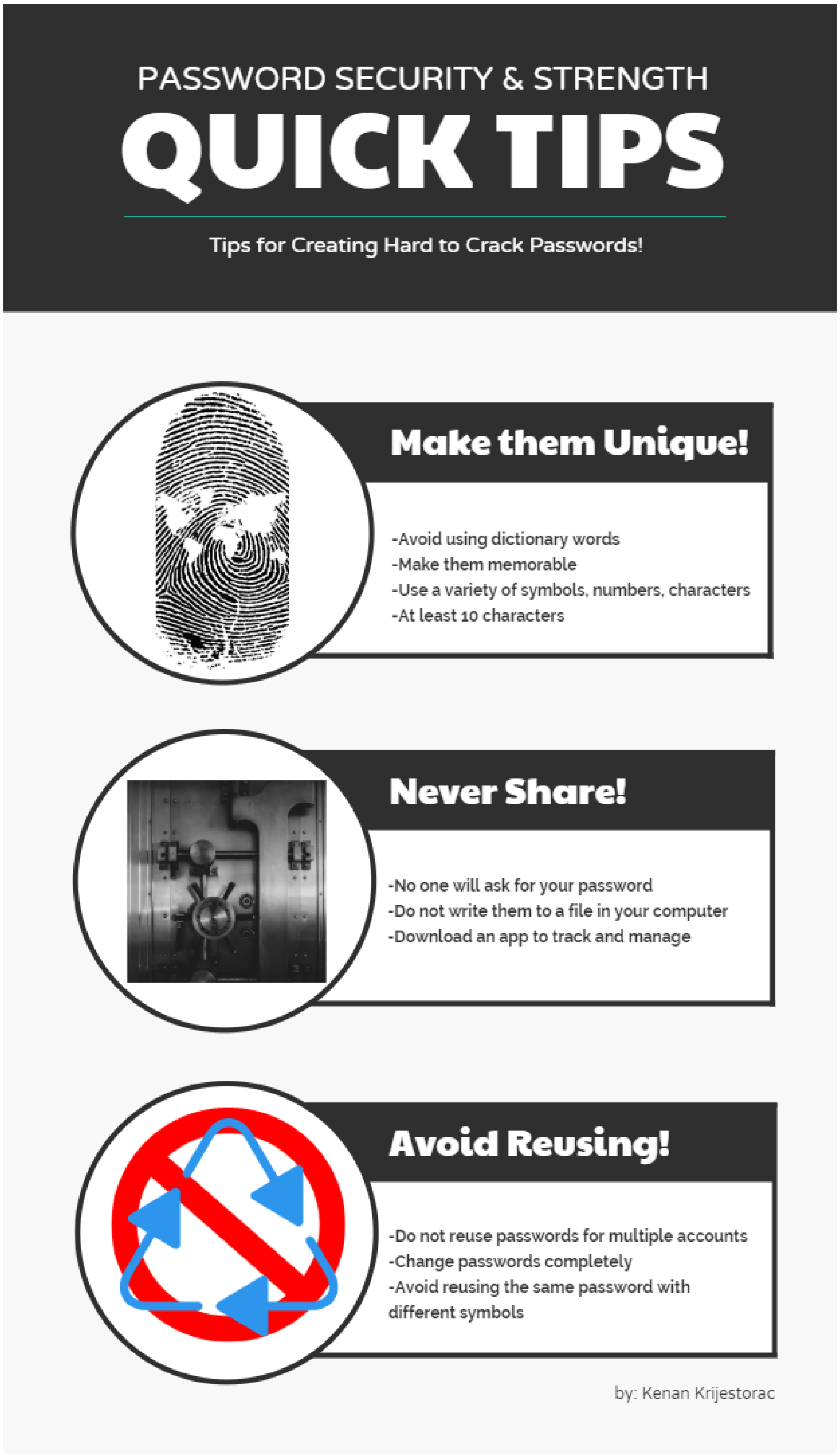
Computer-based Training: The success of the phishing and password training will be measured by the participation of the employees. The average scores of the first will be compared to a pre-determined marker of satisfaction judged by the CIO. The second training will be adjusted to focus on the areas of concern from the trainings from the first half of the year. Additionally, the success of the phishing training will be determined by the results that the simulated phishing attack displays, as well as any potential attacks that the organization faces. Similarly, password training scores will be averaged and compared to the ensuing training in the second half of the year. The success of the password training will be measured against the number of password related attacks that the organization faces throughout the course of the year.

7. PROJECT CHARTER

Project Title	Security Awareness Program
Project Owner	Kenan Krijestorac
Project Sponsor	Jeff Robertson
Estimated Cost	$250,000
Program Launch Date	January 1, 2021
Project Scope	A program will be introduced to all employees to train and raise awareness about phishing/email security and password strength and security. The program is designed to help employees establish skills to identify key details of phishing emails and to develop strong passwords in order to mitigate potential cyber incidents.
Project Goal	Implement an effective and engaging security awareness program in which all employees gain the proper skills to mitigate cyber incidents and ensure compliance with regulations.
Project Deliverables	1. To increase password strength and security through computer-based training. 2. To expand knowledge of general phishing/email security through simulated attacks and training. 3. Mitigate the risks that are a result of lack of awareness. 4. Promote discussion and communication of security topics (phishing and passwords) with brown bag seminars. 5. Conduct surveys on the awareness plan from employee feedback. 6. Generate assessment and progress reports that compare the number of incidents with and without the plan.

Project Justification	The purpose of the security awareness program is to mitigate the risks associated with lack of awareness in common methods of cyber-attacks: phishing and password weakness. As an organization that handles PII and PHI, it is critical in providing an awareness plan that tends to the greatest weakness that our organization faces: human error.
Key Milestones	1. Project Approval 2. Deploy first bi-annual computer-based training for phishing 3. Launch phishing simulation campaign. 4. Determine date for first quarterly brown bag seminar 5. Deploy first bi-annual computer-based training for password security

8. TRAINING AIDS



PASSWORD SECURITY & STRENGTH

QUICK TIPS

Tips for Creating Hard to Crack Passwords!

Make them Unique!

-Avoid using dictionary words
-Make them memorable
-Use a variety of symbols, numbers, characters
-At least 10 characters

Never Share!

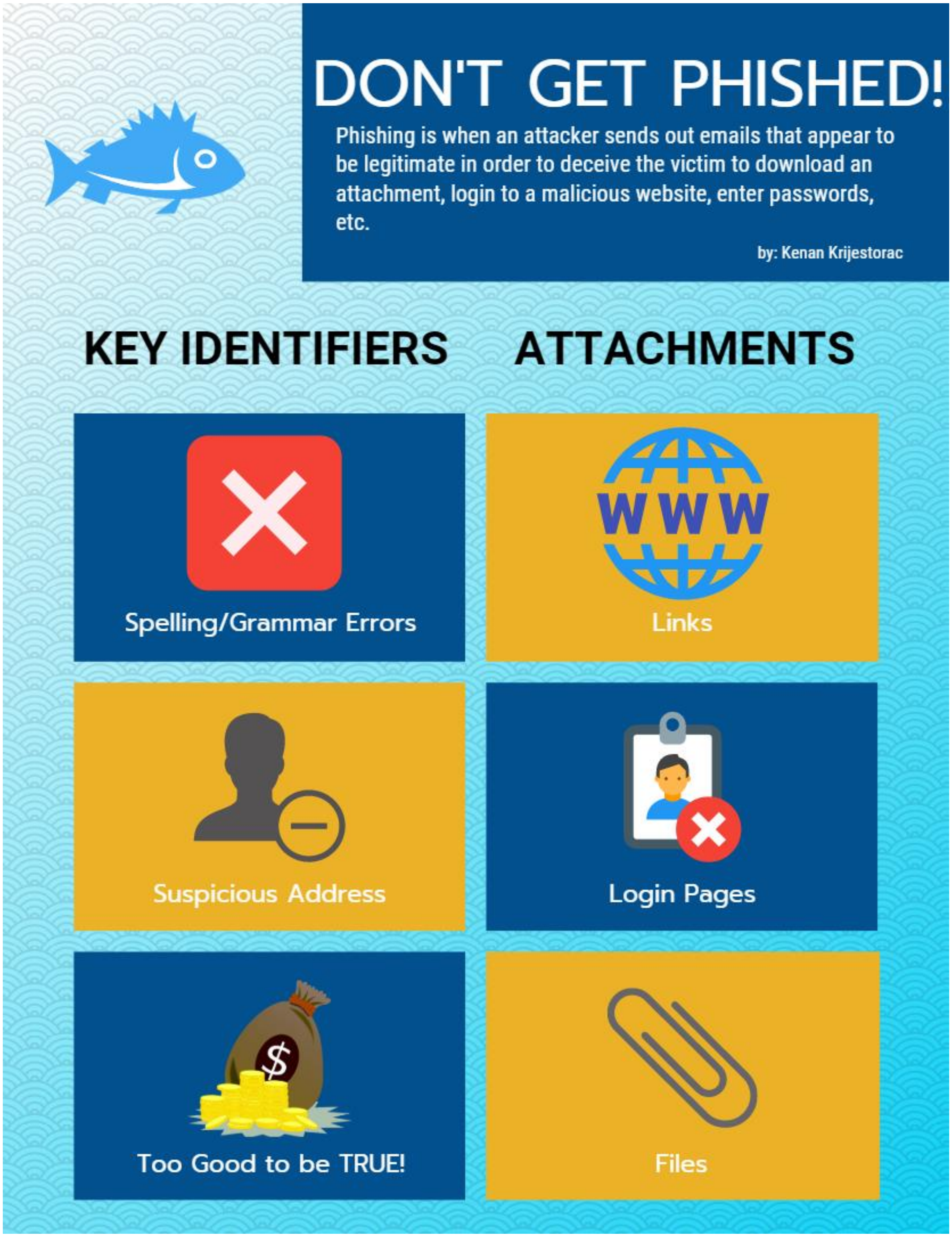
-No one will ask for your password
-Do not write them to a file in your computer
-Download an app to track and manage

Avoid Reusing!

-Do not reuse passwords for multiple accounts
-Change passwords completely
-Avoid reusing the same password with different symbols

by: Kenan Krijestorac

9. TRAINING AIDS



DON'T GET PHISHED!

Phishing is when an attacker sends out emails that appear to be legitimate in order to deceive the victim to download an attachment, login to a malicious website, enter passwords, etc.

by: Kenan Krijestorac

KEY IDENTIFIERS

- Spelling/Grammar Errors
- Suspicious Address
- Too Good to be TRUE!

ATTACHMENTS

- Links
- Login Pages
- Files

10. MAINTENANCE

The security awareness program will be updated and maintained on a year-to-year basis in order to ensure that our employees are receiving the best possible training possible. The first year of deployment will set the pace and success of the years the ensue. The computer-based training for phishing and password security in the second half of the year will be adjusted according to the results of the training in the first half of the year. Employees will be able to offer their feedback on the training itself, and the scores will allow us to assess and update the training for the second half of the year accordingly.

Additionally, training will be updated as new information surfaces about the new versatile phishing methods that hackers are attempting utilize in order to gain access. Similarly, the phishing simulations will be adjusted to reflect the attacks that are being used at the time that it is being deployed.

REFERENCES

Alessandro, K. (2017, June 15). An Achievable Calendar for Cyber Security Plan Implementation. https://www.eci.com/blog/15947-an-achievable-calendar-for-cyber-security-plan-implementation.html

Measuring The Effectiveness of Security Awareness Training. (2018, November 2). https://www.cybsafe.com/blog/measuring-the-effectiveness-of-security-awareness-training/

National Institute of Standards and Technology (2003). Building an Information Technology Security and Awareness Training Program. https://doi.org/10.6028/NIST.SP.800-50

Verizon Enterprise. 2019. *2019 Data Breach Investigations Report.* Retrieved May 1, 2020, from https://www.phishingbox.com/assets/files/images/Verizon-Data-Breach-Investigations-Report-DBIR-2019.pdf >