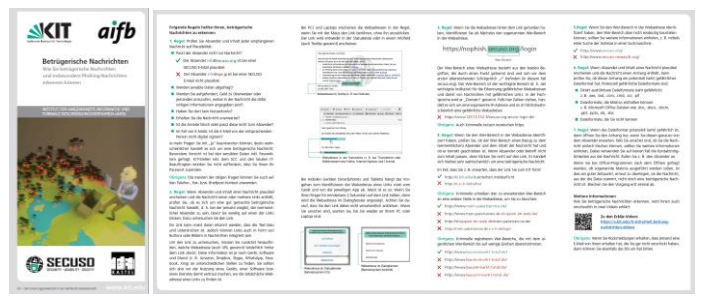
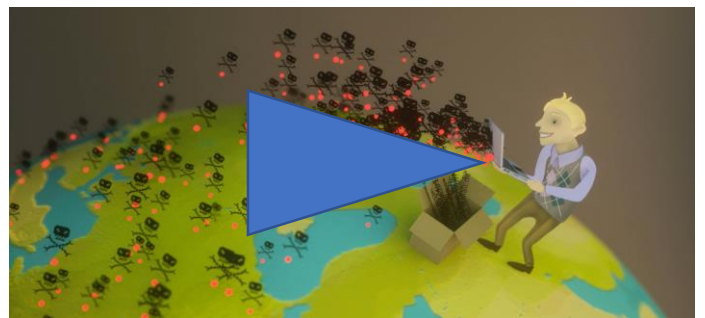


Variante 1: Leichtgewichtiges Programm

Phase 1: Verteilen / zur Verfügung stellen von Basiswissen
 (zwei unterschiedliche Medienform, da jeder andere Vorlieben bei Informationsgewinnung hat)



Flyer = Textform (ca. 15 min)



2 Erklärvideos à 5 min (ca. 10min)

Phase 2: Anwenden des Wissens und Infos zum Nachlesen
 (kurz nach Phase 1: Challenge Poster an diversen Orten aufhängen, Regel-Poster in jedem Büro eins aufhängen lassen)



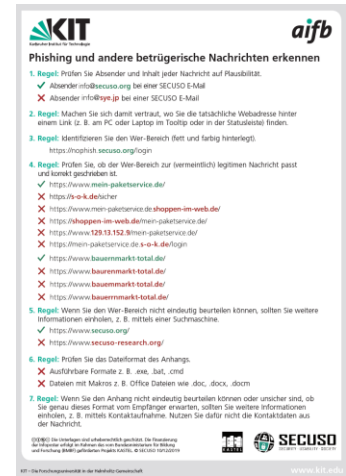
Mehrere Challenge Poster inkl. Webseiten mit Auflösung

Erklär-Poster z.B. neben den Infos zum Verhalten im Brandfall pro Raum aufhängen

Phase 3: Auffrischung
 (nach ca. 6 Monaten: Info-Karte an alle verteilen und Challenge Poster erneuern ggf. bezogen auf wirklich verschickte E-Mail, Anlass z.B. zum Safer Internet Day)



Info-Karte im Hosentaschenformat

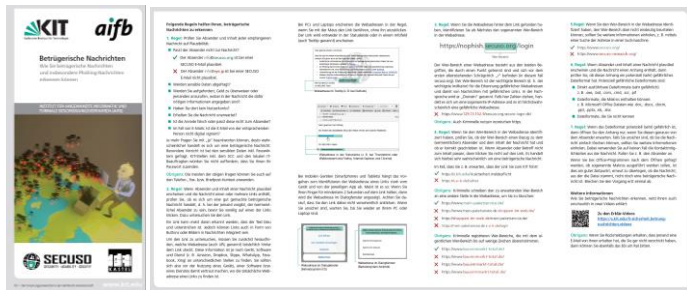


Phase 4 und folgende:
 Wiederholung von Phase 1-3
 (nach ca. weiteren 6 Monaten: ggf. die Challenge Poster als kleines Web-Quiz anbieten, ggf. neue Angriffe aufnehmen)

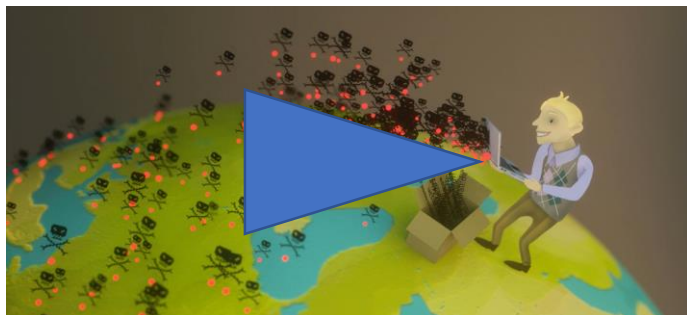


Variante 2: Leichtgewichtiger Start

Phase 1: Verteilen / zur Verfügung stellen von Basiswissen
(zwei unterschiedliche Medienform, da jeder andere Vorlieben bei Informationsgewinnung hat)



Flyer = Textform (ca. 15 min)



2 Erklärvideos à 5 min (ca. 10min)

Phase 2: Anwenden des Wissens und Infos zum Nachlesen
(kurz nach Phase 1: Challenge Poster an diversen Orten aufhängen, Regel-Poster in jedem Büro eins aufhängen lassen)

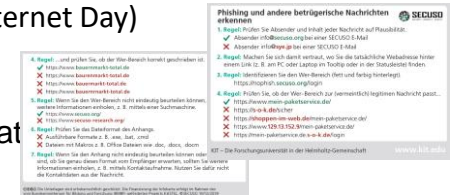


Mehrere Challenge Poster inkl. Webseiten mit Auflösung

Erklär-Poster z.B. neben den Infos zum Verhalten im Brandfall pro Raum aufhängen

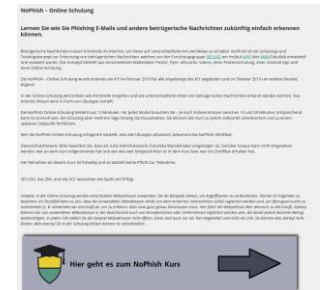
Phase 3: Auffrischung
(nach ca. 6 Monaten: Info-Karte an alle verteilen und Challenge Poster erneuern ggf. bezogen auf wirklich verschickte E-Mail, Anlass z.B. zum Safer Internet Day)

Info-Karte im Hosentaschenformat



Phase 4: Detailwissen inkl. Quizz

(nach ca. weiteren 6 Monaten: Wissen vertiefen und Wissenstand über Quizz erfassen; ggf. in Standards gefordert)



Schulung (ca. 2 Stunden) als E-Learning oder Vortrag

Phase 5 und folgende: Wiederholung von Phase 1-4

(nach ca. weiteren 6 Monaten: ggf. die Challenge Poster als kleines Web-Quiz anbieten, ggf. neue Angriffe aufnehmen)

Variante 3: Erst ausführlich Schulen

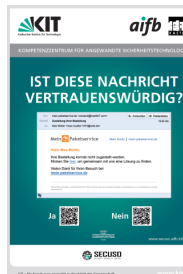
Phase 1: Detailwissen inkl. Quizz
(nach ca. weiteren 6 Monaten: Wissen vertiefen und Wissenstand über Quizz erfassen; ggf. in Standards gefordert)

Phase 2: Anwenden des Wissens und Infos zum Nachlesen
(nach ca. 6 Monaten: Challenge Poster an diversen Orten und Regel-Poster in jedem Büro aufhängen)

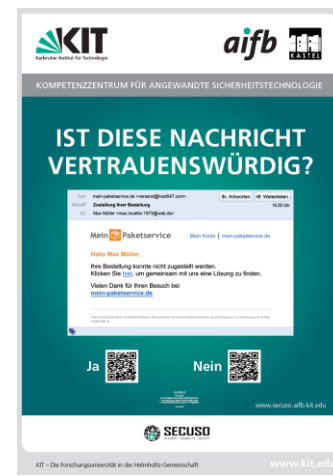
Phase 3: Auffrischung
(nach ca. 6 Monaten: zwei unterschiedliche Medienform, da jeder andere Vorlieben bei Informationsgewinnung hat)

Phase 4: Anwenden des Wissens und Infos zum Nachlesen
(nach ca. 6 Monaten: Info-Karte an alle verteilen und Challenge Poster erneuern ggf. bezogen auf wirklich verschickte E-Mail, Anlass z.B. zum Safer Internet Day)

Info-Karte im Hosentaschenformat



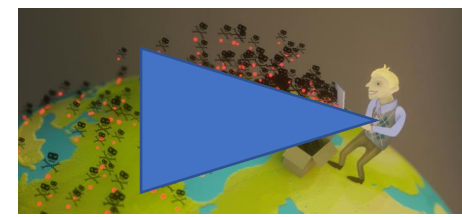
NoPhish - Online Schulung
Lernen Sie wie Sie Phishing E-Mails und andere betrügerische Nachrichten zukünftig einfach erkennen können.
Betrügerische Nachrichten nutzen Kriminelle im Internet, um Ihnen auf unterschiedliche Art und Weise zu schaden. NoPhish ist ein Schulungs- und Trainingskonzept zur Erkennung von betrügerischen Nachrichten, welches von der Forschungsgruppe SECUSO am Institut aifb der KIT-Fakultät entwickelt und evaluiert wurde. Das Konzept besteht aus verschiedenen Materialien: Poster, Flyer, Infocards, Videos, einer Präsenzschiulung, einer Android App und einer Online-Schulung.
Die NoPhish - Online Schulung wurde erstmals am KIT im Februar 2019 für alle Angehörige des KIT angeboten und im Oktober 2019 um weitere Module ergänzt.
In der Online Schulung wird erklärt wie Kriminelle vorgehen und wie unterschiedliche Arten von betrügerischen Nachrichten erkannt werden können. Das erste Wissen wird in Form von Übungen vertieft.
Die NoPhish Online-Schulung besteht aus 12 Modulen. Für jedes Modul brauchen Sie - je nach Vorkenntnissen zwischen 10 und 20 Minuten. Entsprechend kann es sinnvoll sein, die Schulung über mehrere Tage hinweg durchzuführen. Sie können den Kurs zu jedem Zeitpunkt unterbrechen und zu einem späteren Zeitpunkt fortführen.
Wer die NoPhish Online-Schulung erfolgreich besteht, also alle Übungen absolviert, bekommt das NoPhish Zertifikat.
Datenschutzhinweis: Bitte beachten Sie, dass als ILLIAS-Administratorin Franziska Wandelmaier eingetragen ist. Darüber hinaus kann nicht eingesehen werden, wer an dem Kurs teilgenommen hat und wer wie weit fortgeschritten ist in dem Kurs bzw. wer ein Zertifikat erhalten hat.
Die Teilnahme an diesem Kurs ist freiwillig und es besteht keine Pflicht zur Teilnahme.
SECUSO, das ZML und das SCC wünschen viel Spaß und Erfolg.



Mehrere Challenge Poster inkl. Webseiten mit Auflösung



Flyer = Textform (ca. 15 min)



2 Erklärvideos à 5 min (ca. 10min)



Erklär-Poster z.B. neben den Infos zum Verhalten im Brandfall pro Raum aufhängen

Phase 5 und folgende:
Wiederholung von Phase 1-4
(nach ca. weiteren 6 Monaten: ggf. die Challenge Poster als kleines Web-Quiz anbieten statt als Poster aufhängen, ggf. neue Angriffe aufnehmen)



Variante 4: Erst ausführlich Schulen +früh Auffrischen

Phase 1: Detailwissen inkl. Quiz
 (nach ca. weiteren 6 Monaten: Wissen vertiefen und Wissenstand über Quiz erfassen; ggf. in Standards gefordert)

Phase 2: Auffrischung
 (nach ca. 6 Monaten: zwei unterschiedliche Medienform, da jeder andere Vorlieben bei Informationsgewinnung hat)

Phase 3: Anwenden des Wissens und Infos zum Nachlesen
 (nach ca. 6 Monaten: Challenge Poster an diversen Orten und Regel-Poster in jedem Büro aufhängen)

Phase 4: Auffrischung
 (nach ca. 6 Monaten: Wie Phase 2)

Phase 5: Anwenden des Wissens und Infos zum Nachlesen
 (nach ca. 6 Monaten: Info-Karte an alle verteilen und Challenge Poster erneuern ggf. bezogen auf wirklich verschickte E-Mail, Anlass z.B. zum Safer Internet Day)

Info-Karte im Hosentaschenformat

Phase 6 und folgende: Wiederholung von Phase 1-5
 (nach ca. weiteren 6 Monaten: ggf. die Challenge Poster als kleines Web-Quiz anbieten statt als Poster aufhängen, ggf. neue Angriffe aufnehmen)

NoPhish - Online Schulung

Lernen Sie wie Sie Phishing E-Mails und andere betrügerische Nachrichten zukünftig einfach erkennen können.

Betrügerische Nachrichten nutzen Kriminelle im Internet, um Ihnen auf unterschiedliche Art und Weise zu schaden. NoPhish ist ein Schulungs- und Trainingskonzept zur Erkennung von betrügerischen Nachrichten, welches von der Forschungsgruppe SECUSO am Institut aifb (der KIT) entwickelt und evaluiert wurde. Das Konzept besteht aus verschiedenen Materialien: Poster, Flyer, Infocards, Videos, einer Präsenzschiulung, einer Android App und einer Online-Schulung.

Die NoPhish - Online Schulung wurde erstmals am KIT im Februar 2019 für alle Angehörige des KIT angeboten und im Oktober 2019 um weitere Module ergänzt.

In der Online Schulung wird erklärt wie Kriminelle vorgehen und wie unterschiedliche Arten von betrügerischen Nachrichten erkannt werden können. Das gesamte Wissen wird in Form von Übungen vertieft.

Die NoPhish Online-Schulung besteht aus 12 Modulen. Für jedes Modul brauchen Sie - je nach Vorkenntnissen zwischen 10 und 20 Minuten. Entsprechend kann es sinnvoll sein, die Schulung über mehrere Tage hinweg durchzuführen. Sie können den Kurs zu jedem Zeitpunkt unterbrechen und zu einem späteren Zeitpunkt fortführen.

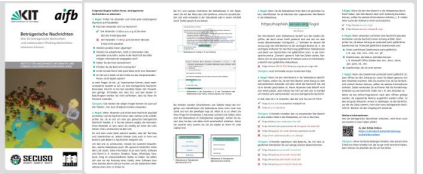
Wer die NoPhish Online-Schulung erfolgreich besteht, also alle Übungen absolviert, bekommt das NoPhish Zertifikat.

Datenschutzhinweis: Bitte beachten Sie, dass als ILIAS-Administratorin Franziska Wandelmaier eingetragen ist. Darüber hinaus kann nicht eingesehen werden, wer an dem Kurs teilgenommen hat und wer wie weit fortgeschritten ist in dem Kurs bzw. wer ein Zertifikat erhalten hat.

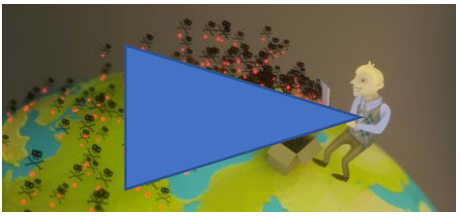
Die Teilnahme an diesem Kurs ist freiwillig und es besteht keine Pflicht zur Teilnahme.

SECUSO, das ZIM und das SCC wünschen viel Spaß und Erfolg!

Hinweis: In der Online Schulung werden verschiedene Webadressen verwendet, die als Beispiele dienen, um Angriffsarten zu verdeutlichen. Hierbei ist folgendes zu beachten: Die Erstellung kann es sein, dass die verwendeten Webadressen direkt von dem jeweiligen Unternehmen selbst registriert werden sind, um Betrügern die Unterscheidung zu erleichtern (z. B. verwenden wir microsoft.de, um zu erklären, dass man ganz genau hinschauen muss. Hier führt die Webadresse über dennoch zu Microsoft, ebenso können von uns verwendete Webadressen in der Zwischenzeit auch von Einzelpersonen oder Unternehmen registriert worden sein, die damit jedoch keinerlei Bezug zum Original haben. In jedem Fall sollten Sie die Beispiel Webadressen nicht öffnen, diese sind auch nur als Text eingegeben und nicht als Link. Sie können also darauf nicht klicken. Alles worauf Sie in der Schulung klicken können ist unbedenklich.



Flyer = Textform (ca. 15 min)



2 Erklärvideos à 5 min (ca. 10min)



Erklär-Poster z.B. neben den Infos zum Verhalten im Brandfall pro Raum aufhängen

Mehrere Challenge Poster inkl. Webseiten mit Auflösung

KIT aifb SECUSO

Phishing und andere betrügerische Nachrichten erkennen

- Regel:** Prüfen Sie Absender und Inhalt jeder Nachricht auf Plausibilität.
 - ✓ Absender info@secuso.org bei einer SECUSO E-Mail
 - ✗ Absender info@bayer.de bei einer SECUSO E-Mail
- Regel:** Machen Sie sich damit vertraut, wo Sie die tatsächliche Webadresse hinter einen Link (z. B. am PC oder Laptop im Kopfbereich oder in der Statusleiste) finden.
- Regel:** Identifizieren Sie den Web-Bereich zur (vermeintlich) legitimen Nachricht.
 - https://phishing.secuso.org/login
 - https://www.mein-paketservice.de/ ✓
 - https://www-mein-paketservice.de/ ✗
 - https://www-mein-paketservice.de/abgeben-im-web.de/ ✗
 - https://abgeben-im-web.dahlem-paketservice.de/ ✗
 - https://www.12313152.mein-paketservice.de/ ✗
 - https://mein-paketservice.de/s-o-k.de/login ✓
 - https://www.bawermarks-total.de/ ✓
 - https://www.bawermarks-total.de/ ✗
 - https://www.bawermarks-total.de/ ✗
 - https://www.bawermarks-total.de/ ✗
- Regel:** Wenn Sie den Web-Bereich nicht eindeutig beurteilen können, sollten Sie weitere Informationen einholen, z. B. mittels einer Suchmaschine.
 - https://www.secuso.org/ ✓
 - https://www.secuso.org/aifb/ ✓
- Regel:** Prüfen Sie das Dateiformat des Anhangs.
 - ✗ Ausführbare Formate z. B. exe, bat, cmd
 - ✗ Dateien mit Klärsatz z. B. Office-Dateien wie doc, docx, docm
- Regel:** Wenn Sie den Anhang nicht eindeutig beurteilen können oder unsicher sind, ob Sie genau dieses Format vom Empfänger erwarten, sollten Sie weitere Informationen einholen, z. B. mittels Kontaktaufnahme. Nutzen Sie dafür nicht die Kontaktdaten aus der Nachricht.

(SECUSO) Die Inhalte sind urheberrechtlich geschützt. Die Weitergabe der Inhalte erfolgt auf Anfrage des nachfolgenden Betriebs und nach Prüfung durch den jeweiligen Projektleiter. © KIT 2019 10/2019

Phishing und andere betrügerische Nachrichten erkennen

- Regel:** Prüfen Sie Absender und Inhalt jeder Nachricht auf Plausibilität.
 - ✓ Absender info@secuso.org bei einer SECUSO E-Mail
 - ✗ Absender info@bayer.de bei einer SECUSO E-Mail
- Regel:** Machen Sie sich damit vertraut, wo Sie die tatsächliche Webadresse hinter einen Link (z. B. am PC oder Laptop im Kopfbereich oder in der Statusleiste) finden.
- Regel:** Identifizieren Sie den Web-Bereich zur (vermeintlich) legitimen Nachricht.
 - https://phishing.secuso.org/login
 - https://www.mein-paketservice.de/ ✓
 - https://www-mein-paketservice.de/ ✗
 - https://www-mein-paketservice.de/abgeben-im-web.de/ ✗
 - https://abgeben-im-web.dahlem-paketservice.de/ ✗
 - https://www.12313152.mein-paketservice.de/ ✗
 - https://mein-paketservice.de/s-o-k.de/login ✓
 - https://www.bawermarks-total.de/ ✓
 - https://www.bawermarks-total.de/ ✗
 - https://www.bawermarks-total.de/ ✗
 - https://www.bawermarks-total.de/ ✗
- Regel:** Wenn Sie den Web-Bereich nicht eindeutig beurteilen können, sollten Sie weitere Informationen einholen, z. B. mittels einer Suchmaschine.
 - https://www.secuso.org/ ✓
 - https://www.secuso.org/aifb/ ✓
- Regel:** Prüfen Sie das Dateiformat des Anhangs.
 - ✗ Ausführbare Formate z. B. exe, bat, cmd
 - ✗ Dateien mit Klärsatz z. B. Office-Dateien wie doc, docx, docm
- Regel:** Wenn Sie den Anhang nicht eindeutig beurteilen können oder unsicher sind, ob Sie genau dieses Format vom Empfänger erwarten, sollten Sie weitere Informationen einholen, z. B. mittels Kontaktaufnahme. Nutzen Sie dafür nicht die Kontaktdaten aus der Nachricht.

(SECUSO) Die Inhalte sind urheberrechtlich geschützt. Die Weitergabe der Inhalte erfolgt auf Anfrage des nachfolgenden Betriebs und nach Prüfung durch den jeweiligen Projektleiter. © KIT 2019 10/2019

