

Phishing: den Fang verhindern

In dieser Unterrichtseinheit werden Schülerinnen und Schüler mit dem Phishing (Kurzform für Password-Fishing) konfrontiert. Mit diesem Kunstwort wird der Trick bezeichnet, mithilfe gefälschter E-Mails an vertrauliche, persönliche Daten zu gelangen.

Die Verbreitung so genannter Phishing-Mails steigt rasant an. Nutzerinnen und Nutzer werden darin aufgefordert, Namen und Bankverbindungen preiszugeben und diese Daten zu versenden. Phisher versenden E-Mails, in denen zum Beispiel Bankkunden zu einem "Sicherheitscheck" aufgefordert werden. Die Mails enthalten Links zu gefälschten Webseiten, die der Original-Website des Geldinstituts zum Verwechseln ähnlich sehen. Dort werden die Kunden aufgefordert, ihre persönliche Geheimnummer (PIN) und die so genannte Transaktionsnummer (TAN) einzugeben. Die Schülerinnen und Schüler werden in dieser Stunde mit der Vorgehensweise der "Phisher" vertraut gemacht und somit für derartige Betrugsversuche sensibilisiert. Dieses Thema ist nicht nur gegenwärtig, sondern auch zukünftig von Bedeutung, da Betrüger immer wieder das Internet für ihre Zwecke nutzen werden. Somit steht der Lerninhalt exemplarisch für die Schulung des Sicherheitsdenkens im Umgang mit dem Internet wie auch generell mit personenbezogenen Daten.

Lernziele

Die Schülerinnen und Schüler sollen

- § Sicherheits- und Echtheitsmerkmale von Webseiten und E-Mails kennen lernen
- § durch die Darstellung einer Phishing-Mail diese als Betrugsversuch erkennen können
- § wissen, wie eine Phishing-Attacke generell abläuft und wie man sich davor schützen kann
- § das Internet als Informationsquelle nutzen und die benötigten Informationen auswählen
- § die Informationen strukturieren und gliedern

Kurzinformation

Thema	Phishing verhindern: Sicherheitsmerkmale von E-Mails und Webseiten
Autor	Markus Czehak
Fach	Datenverarbeitung
Zielgruppe	Sekundarstufe II
Zeitraum	eine Unterrichtsstunde
Technische Voraussetzungen	Beamer, ein Computer pro Schüler(in)

Verlaufsplan der Unterrichtseinheit

Phase	Inhalt	Sozial- / Aktionsform	Medien / Dateien
Einstieg/Motivation	E-Mail der Rastbank fordert zu einem Sicherheitscheck auf; Erläuterung der E-Mail und der Situation (Bank gewechselt, Online-Banking, jetzt E-Mail erhalten mit Hinweis auf Sicherheitscheck)	Impuls, Unterrichtsgespräch	Beamer, E-Mail "Rastbank"
Problemwahrnehmung	Eventuell Begriffe PIN und TAN besprechen. E-Mail und (gefälschte) Website der Rastbank "Ist die Webseite der Rastbank echt?" "Wie kann sichergestellt werden, dass die Webseite "echt" ist?" Echtheitsmerkmale einer Website.	Schülergespräch, impulsgeleitet	Beamer, E-Mail und Website
Problementfaltung	E-Mail und Website Lernende stellen Vermutungen über Echtheit der E-Mail an Link in der E-Mail wird thematisiert Eventuell Unterstützung durch Arbeitstransparent. Echtheitsmerkmale auf Flipchart notieren. Problem: Website offensichtlich gefälscht, E-Mail aber anscheinend echt	Schülergespräch, impulsgeleitet	Beamer, E-Mail und Website Flipchart
Informationserarbeitung	Lernende erhalten Arbeitsaufträge, um Fragen rund um das Phishing zu klären.	Gruppenarbeit	Arbeitsaufträge Internet
Sicherung	Lernende präsentieren ihre Ergebnisse auf Folien (Arbeitsaufträge auf Folie kopieren),	Schülergespräch, impulsgeleitet	OHP, Arbeitstransparent "Arbeitsaufträge"

	Zusammenfassung der Ergebnisse, evtl. abschließende Beurteilung der Sicherheit von Online-Banking		
--	---	--	--

Didaktisch-methodischer Kommentar

Ausgehend von einer echten Phishing-Mail und einer auf dem Server hinterlegten gefälschten Webseite der "Rastbank" sollen die Lernenden spontan äußern, was ihrer Meinung nach Merkmale sind, an denen sich die Echtheit einer Webseite und einer E-Mail zeigen.

Hier ist zu erwarten, dass die Lernenden einerseits die URL, andererseits den Absender einer E-Mail nennen werden. Daraus folgt, dass die gezeigte E-Mail echt sein müsste und die Webseite demnach eine Fälschung. Da die vermeintlich echte E-Mail auf die gefälschte Webseite verweist, ergibt sich für die Lernenden ein Widerspruch. Diesen gilt es durch die Informationsrecherche im Internet aufzulösen.

<http://lo-net2.de/group/Material/01%20Einstieg%20Rastbank.html>

Wir haben die Dateien hier beispielhaft auf dem lo-net-Server abgelegt.

Da die E-Mail einen Link enthält, wird auch thematisiert, woran zu erkennen ist, auf welche Webseite ein Link führt. Durch die Internetrecherche wird nachgewiesen, dass ein solcher Link nicht zuverlässig ist. Die Lernenden erhalten ausgewählte Internetadressen, da eine eigenständige Recherche nicht in einer einzelnen Unterrichtsstunde zu bewältigen ist. Jeder Arbeitsauftrag umfasst zwei bis drei Teilaufgaben, so dass sich die Lernenden in der Gruppe hinsichtlich der Aufgabenverteilung und der Ergebniszusammenführung abstimmen müssen.

Abschließend werden die Ergebnisse der Gruppen präsentiert. Da es sich um eine arbeitsteilige Gruppenarbeit handelt, sollen die Lernenden nach der Präsentation Vorschläge machen, wie die Ergebnisse allen zur Verfügung gestellt werden können.

Benötigte Dateien:

[Arbeitsblatt_Phishing.rtf](#)

[Arbeitsblatt_Phishing_Loesungen.rtf](#)

[Rastbank.zip](#): Hier befindet sich die Datei 01EinstiegRastbank.html sowie die Datei RastbankLogin.htm mit diversen Grafiken im separaten Ordner für die E-Mail und offensichtlich gefälschte Website einer imaginären Bank (Rastbank).

Zusatzinformationen

im WWW

<http://idw-online.de/pages/de/news90358>

„Oft zu wenig Phishing-Schutz bei Online-Banken“ - eine Pressemitteilung des Fraunhofer-Instituts für Sichere Informationstechnologie.

<http://www.heise.de/tp/r4/artikel/18/18805/1.html>

Online-Artikel „Aufrüstung der Cyber-Kriminellen“ bei heise.de.

<http://www.wiwo.de/pswiwo/fn/ww2/sfn/buildww/id/133/id/76477/fm/0/bt/2/SH/0/depot/0/>

IT-Sicherheit: Auf Phishzug. Online-Artikel bei wiwo.de.

bei Lehrer-Online

<http://www.lehrer-online.de/url/e-mail-verschluesseln>

Eine Unterrichtseinheit, die sich um das Verschlüsseln von E-Mails mit Pretty Good Privacy und GnuPG dreht.

Informationen zum Autor

Markus Czehak unterrichtet Wirtschaftsinformatik am Berufskolleg für Wirtschaft und Informatik in Neuss.