(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년03월31일
(11) 등록번호 10-1722279
(24) 등록일자 2017년03월27일

(51) 국제특허분류(Int. Cl.)
G06Q 50/32 (2012.01)
(21) 출원번호 10-2011-7027967
(22) 출원일자(국제) 2010년05월18일
심사청구일자 2015년04월21일
(85) 번역문제출일자 2011년11월23일
(65) 공개번호 10-2012-0027264
(43) 공개일자 2012년03월21일
(86) 국제출원번호 PCT/US2010/035202
(87) 국제공개번호 WO 2010/138339
국제공개일자 2010년12월02일
(30) 우선권주장
12/472,094 2009년05월26일 미국(US)
(56) 선행기술조사문헌
US06052709 A
US06161130 A
US20070157113 A1

(73) 특허권자
마이크로소프트 테크놀로지 라이센싱, 엘엘씨
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
바이티링암 간디
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 어텐션: 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
호 쳉
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 어텐션: 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
(뒷면에 계속)
(74) 대리인
제일특허법인

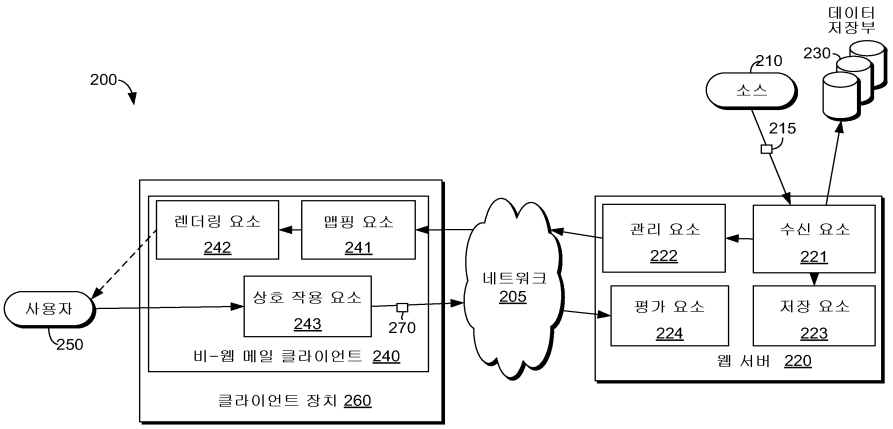
전체 청구항 수 : 총 20 항 심사관 : 이원재

(54) 발명의 명칭 **비-웹 메일 클라이언트 콘텍스트 내 잠재적 피싱 메시지들의 관리**

(57) 요 약

통신이 잠재적 피싱 이메일이라는 것을 식별한 직후에 디지털 통신물들(예를 들면 이메일들과 인스턴트 메시지들)의 처리를 관리하는 컴퓨터화된 방법들과 컴퓨터 판독 가능 매체가 제공된다. 통신의 의도된 수신자에게 배정된 계정의 거동을 제어하기 위해서 서비스 제공자가 이용된다. 계정의 거동의 제어는 서비스 제공자에 의해서 다이내믹하게 설정되지 않는 UI 디스플레이를 렌더링하는 비-웹 메일 서버의 맥락에서 서술된다. 한 해결책에서, 거동의 제어는 이들 통신들을 분리된 폴더에 모으는 방식에 의해 사용자에게 잠재적 피싱으로 식별된 통신들의 존재를 알린다. 다른 해결책에서, 거동의 제어는 잠재적 피싱 통신의 콘텐츠를 경고 메시지로 대체하는 방식에 의해 사용자 보호를 용이하게 한다. 이 경고 메시지는 사용자가 잠재적 피싱 통신들의 본래 콘텐츠를 볼 수 있는 웹 브라우저에 대한 URL 링크를 선택적으로 포함한다.

대 표 도



(72) 발명자

피티고이-아론 그루이아

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 어텐션: 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

빈센트 벤

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 어텐션: 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

명 세 서

청구범위

청구항 1

실행시에, 사용자가 비-웹 메일 클라이언트(non-web mail client)를 통해 계정에 액세스하는 경우 상기 사용자에게 잠재적 피싱 이메일(potentially phishing email)을 통지하는(alerting) 방법을 수행하는 컴퓨터 실행가능 명령어들을 포함하는 하나 이상의 컴퓨터 판독가능 장치로서,

상기 방법은

상기 사용자와 연관된 상기 비-웹 메일 클라이언트에서 디지털 통신물(digital communication)을 수신하는 단계 - 상기 비-웹 메일 클라이언트는 서비스 제공자와는 연관이 없음 -와,

상기 디지털 통신물을 잠재적 피싱 이메일로서 식별한 후에, 상기 디지털 통신물에 메타데이터 태그를 첨부하는 단계와,

잠재적 피싱 이메일로 식별된 디지털 통신물의 유지를 전담하는 제1 저장 장소 내에 상기 태그된 디지털 통신물을 위치시키는 단계- 상기 제1 저장 장소는 정당한 것으로 식별된 디지털 통신물을 유지하는 제2 저장 장소와는 별개인 물리적 메모리 장소를 제공함 -와,

상기 사용자가 상기 비-웹 메일 클라이언트를 통해서 상기 계정에 액세스하는 경우 상기 사용자에게 상기 제1 저장 장소의 시각적 표현을 표시하는 단계- 상기 시각적 표현은 하나 이상의 잠재적 피싱 이메일이 상기 사용자의 계정에 도착했다는 표시를 상기 사용자에게 제공함 -

를 포함하는

컴퓨터 판독가능 장치.

청구항 2

제 1 항에 있어서,

상기 방법은 상기 잠재적 피싱 이메일로서 식별된 상기 디지털 통신물과 연관된 상기 첨부된 태그를 상기 하나 이상의 컴퓨터 판독가능 장치 상의 격리 목록에 유지하는 단계를 더 포함하고, 상기 격리 목록은 상기 사용자의 계정에 도착한 상기 하나 이상의 잠재적 피싱 이메일 각각을 나열하는

컴퓨터 판독가능 장치.

청구항 3

제 1 항에 있어서,

상기 방법은 상기 디지털 통신물이 상기 잠재적 피싱 이메일인지 여부를 확인하기 위해서 필터링 휴리스틱(filtering heuristics)을 적용하는 단계를 더 포함하고, 상기 잠재적 피싱 이메일은 상기 사용자로 하여금 개인 정보를 누설하도록 부정하게 요청하는 메시지인

컴퓨터 판독가능 장치.

청구항 4

제 3 항에 있어서,

상기 방법은 상기 디지털 통신물이 상기 잠재적 피싱 이메일인 것으로 확인되면 상기 제1 저장 장소를 생성하는

단계를 더 포함하는

컴퓨터 판독가능 장치.

청구항 5

제 1 항에 있어서,

상기 디지털 통신물은 이메일 메시지 및 인스턴트 메시지 중 적어도 하나를 포함하고, 상기 디지털 통신물은 상기 하나 이상의 컴퓨터 판독가능 장치로부터 제거된 소스로부터 수신되는

컴퓨터 판독가능 장치.

청구항 6

제 1 항에 있어서,

상기 비-웹 메일 클라이언트는 사용자 인터페이스(UI) 디스플레이를 상기 사용자에게 렌더링함으로써 상기 사용자에게 상기 계정에 대한 액세스를 제공하고, 상기 UI 디스플레이 상에서 공개되는 요소들은 상기 사용자 계정을 관리하는 상기 서비스 제공자에 의해서 제어되지 않는

컴퓨터 판독가능 장치.

청구항 7

제 6 항에 있어서,

상기 방법은 상기 잠재적 피싱 이메일에 대해 동작을 실행하도록 상기 UI 디스플레이를 통해 상기 사용자에 의해 개시된 요청을 가로채는 단계를 더 포함하는

컴퓨터 판독가능 장치.

청구항 8

제 7 항에 있어서,

상기 방법은

상기 디지털 통신물에 첨부된 상기 메타데이터 태그를 검사함으로써 상기 사용자 개시 요청이 상기 잠재적 피싱 이메일로 식별된 상기 디지털 통신물을 향한 것임을 확인하는 단계와,

상기 요청 내에서 전달된 상기 동작이 제한된 동작인지 여부를 확인하는 단계

를 더 포함하는

컴퓨터 판독가능 장치.

청구항 9

제 8 항에 있어서,

상기 방법은

상기 사용자 개시 요청이 상기 잠재적 피싱 이메일로서 식별된 상기 디지털 통신물을 향한 것이고 상기 요청 내에서 전달된 상기 동작이 제한된 동작임을 확인한 경우, 상기 동작의 실행을 방지하는 단계와,

상기 요청에 대한 응답으로 상기 비-웹 메일 클라이언트에게 작업-실패 표시를 전송하는 단계

를 더 포함하는

컴퓨터 판독가능 장치.

청구항 10

제 9 항에 있어서,

상기 제한된 동작은 회신 명령, 모두에 회신 명령(reply to all command) 및 전달 명령 중 적어도 하나를 포함하는

컴퓨터 판독가능 장치.

청구항 11

제 7 항에 있어서,

상기 동작은 상기 디지털 통신물을 상기 제1 저장 장소로부터 상기 제2 저장 장소로 이동시키려 시도하는 명령을 포함하고,

상기 방법은

상기 동작이 상기 이동 시도 명령임을 확인하는 단계와,

상기 제1 저장 장소 밖으로의 상기 디지털 통신물의 이동을 허용하지 않는 단계를 더 포함하는

컴퓨터 판독가능 장치.

청구항 12

제 1 항에 있어서,

상기 방법은

상기 제1 저장 장소의 상기 시각적 표현을, 상기 비-웹 메일 클라이언트에 의해 렌더링되는 UI 디스플레이 상에 폴더로서 표시하는 단계와,

상기 폴더의 선택을 수신하면, 상기 사용자의 계정에 도착하였고 상기 제1 저장 장소에 유지되는 상기 하나 이상의 잠재적 피싱 이메일의 표현을 표시하는 단계

를 더 포함하는 컴퓨터 판독가능 장치.

청구항 13

제 12 항에 있어서,

상기 방법은

상기 제1 저장 장소 내에 유지되는 상기 하나 이상의 잠재적 피싱 이메일의 콘텐츠 내에 포함된 URL(uniform-resource locator) 링크들을 비활성화하는 단계와,

상기 하나 이상의 잠재적 피싱 이메일의 표현들의 선택을 수신하는 단계와,

상기 하나 이상의 선택된 잠재적 피싱 이메일의 콘텐츠를 렌더링을 위해서 상기 비-웹 메일 클라이언트에 전달하는 단계

를 더 포함하는

컴퓨터 판독가능 장치.

청구항 14

서버상에 수용된 서비스 제공자에 의해 구현되며, 하나 이상의 디지털 통신물이 비-웹 메일 클라이언트를 통해 액세스되는 경우 상기 하나 이상의 디지털 통신물의 처리를 관리하는 컴퓨터화된 방법으로서,

상기 디지털 통신물의 의도된 수신자와 연관된 상기 비-웹 메일 클라이언트에서 상기 디지털 통신물을 수신하는 경우, 상기 디지털 통신물이 초대받지 않은 메시지인지 또는 정당한 메시지인지 여부를 판단하기 위해서 필터링 휴리스틱을 적용하는 단계- 상기 비-웹 메일 클라이언트는 상기 서비스 제공자와는 연관이 없음 -와,

상기 디지털 통신물이 초대받지 않은 메시지로 판단된 경우, 상기 디지털 통신물을 위험하다고 표시하는 단계와,

상기 위험한 디지털 통신물을 경고 메시지로 대체하는 단계- 상기 위험한 디지털 통신물의 콘텐츠는 상기 경고 메시지 내에 드러나지 않음 -와,

사용자 인터페이스(UI) 디스플레이 내에 렌더링된 목록 내에 상기 경고 메시지의 표현을 표면화할 것을 상기 비-웹 메일 클라이언트에게 지시하는 단계- 상기 목록은 정당한 메시지인 것으로 판단된 하나 이상의 디지털 통신물의 표현을 포함하고, 상기 비-웹 메일 클라이언트에 의해 렌더링된 상기 UI 디스플레이는 상기 사용자의 계정을 관리하는 상기 서비스 제공자에 의해 재구성될 수 없음 -와,

상기 경고 메시지의 표현의 사용자-개시 선택을 수신하는 경우, 상기 경고 메시지를 상기 수신자에게 표시하고 상기 위험한 디지털 통신물의 콘텐츠 공개를 보류하도록 하는 명령어를 상기 비-웹 메일 클라이언트에게 전달하는 단계- 상기 경고 메시지는 상기 위험한 디지털 통신물의 콘텐츠를 액세스하는 것에 관한 지침을 제공함 -

를 포함하는

컴퓨터화된 방법.

청구항 15

제 14 항에 있어서,

정당한 통신물인 것으로 판단된 하나 이상의 디지털 통신물을 보유하는 저장 장소에 상기 위험한 디지털 통신물을 유지하는 단계를 더 포함하는

컴퓨터화된 방법.

청구항 16

제 14 항에 있어서,

상기 경고 메시지는 상기 위험한 디지털 통신물이 잠재적 피싱 이메일로 식별되었다는 통지를 전달하는

컴퓨터화된 방법.

청구항 17

제 14 항에 있어서,

상기 경고 메시지는 선택시에 상기 수신자가 상기 위험한 디지털 통신물의 콘텐츠에 액세스하는 것을 허용하는 웹브라우저에 대한 URL 링크를 포함하는

컴퓨터화된 방법.

청구항 18

실행시에, 비-웹 메일 클라이언트에 의해 렌더링된 사용자 인터페이스(UI) 디스플레이를 통해, 사용자의 계정에 잠재적 피싱 이메일이 도착했음을 상기 사용자에게 통지하는 방법을 수행하는 컴퓨터 실행가능 명령어들을 포함하는 하나 이상의 컴퓨터 판독가능 장치로서,

상기 방법은

잠재적 피싱 이메일로서 식별된 하나 이상의 디지털 통신물의 유지를 전담하는 제1 저장 장소를 생성하는 단계- 상기 제1 저장 장소는 정당한 것으로 식별된 디지털 통신물을 유지하는 제2 저장 장소와는 별개인 물리적 메모리 장소를 제공함 -와,

상기 UI 디스플레이 내에 제1 폴더를 렌더링할 것을 상기 비-웹 메일 클라이언트에게 지시하는 단계- 상기 제1 폴더는 상기 제1 저장 장소에 맵핑되고, 상기 비-웹 메일 클라이언트는 서비스 제공자와는 연관이 없음 -와,

상기 제1 폴더에 액세스하기 위해 상기 사용자에 의해 구현된 표시를 검출하는 단계와,

상기 하나 이상의 식별된 디지털 통신물의 표현을 렌더링할 것을 상기 비-웹 메일 클라이언트에게 지시하는 단계- 상기 표현은 상기 하나 이상의 식별된 디지털 통신물의 콘텐츠와 관련된 메타데이터를 포함함 - 를 포함하는

컴퓨터 판독가능 장치.

청구항 19

제 18 항에 있어서,

상기 UI 디스플레이 내에 제1 폴더를 렌더링할 것을 상기 비-웹 메일 클라이언트에게 지시하는 단계는 상기 잠재적 피싱 이메일이 정당한 이메일과 시각적으로 구별되도록, 상기 정당한 이메일로서 식별된 상기 디지털 통신물을 유지하는 상기 제2 저장 장소에 맵핑되는 제2 폴더를 포함하는 목록에 상기 제1 폴더를 렌더링할 것을 상기 비-웹 메일 클라이언트에 지시하는 단계를 포함하는

컴퓨터 판독가능 장치.

청구항 20

제 18 항에 있어서,

상기 방법은

상기 하나 이상의 식별된 디지털 통신물에 대해 상기 사용자에 의해 개시된 동작을 수신하는 단계와,

상기 동작이 수행되지 않게 함으로써 상기 사용자 개시 동작이 실패하게 하는 단계와,

상기 비-웹 메일 클라이언트에게 작업-실패 표시를 전송하는 단계- 상기 작업 실패 표시는 상기 동작의 실패를 통보함 -

를 더 포함하는

컴퓨터 판독가능 장치.

발명의 설명

배 경 기 술

[0001] 서비스 제공자들로 하여금 다양한 소스들로부터 메시지(예를 들면 이메일들, SMS 메시지들, 등)를 수신하고 처리할 수 있게 하고 사용자로 하여금 그들 메시지들을 보고 행동을 취할 수 있게 하는 다양한 기술들이 존재한다. 가끔, 소스들은 범죄 또는 불법적인 컴퓨터 프로그램들과 같이 부정하게 사용자의 개인 정보 공개를

유도하는 메시지들을 사용자에게 전송하는 범죄적 엔티티들(entities)일 수 있다. 부정한 메시지들을 통해서 정보의 공개를 유도하는 과정은 통상 피싱(phishing)이라고 지칭된다. 종종, "피싱"은 전자 통신 내에서 신뢰성 있는 엔티티로 가장하는 방식으로 민감한 정보의 취득을 시도하는 범죄적으로 부정한 프로세스로 특징지어진다; 따라서, 의심하지 않는 사용자로 하여금 본래는 신중한 정보(예를 들면 사용자 이름, 패스워드, 크레디트 카드 정보 등)를 제공하도록 유혹한다. 일부 경우들에서, 피싱은 사용자에게 적법한 이메일 또는 인스턴트 메시지와 유사한 모습과 느낌을 가지는 이메일 또는 인스턴트 메시지를 보내서 사용자로 하여금 가짜 웹사이트(즉 은행을 패러디한 웹사이트)를 탐색하도록 안내하고, 사용자가 가짜 웹사이트에서 개인 정보(예를 들면 뱅크 계정 로그온, 사용자 식별 정보, 주민 등록 번호 등)를 입력하도록 미끼를 놓는 방식으로 수행된다.

[0002] 서비스 제공자들은 이들 피싱 메시지들을 식별하기 위한 조치를 취하고 있다. 더 나아가, 만약에 서비스 제공자들이 메시지를 피싱 메시지로 식별했다면, 서비스 제공자들은 피싱 메시지에 의해 잠재적으로 초래될 피해의 최소화를 시도할 수 있다. 그러나 서비스 제공자와 연관되지 않은 클라이언트-측 애플리케이션(client-side application)이 사용자 계정 내 메시지들을 접속하기 위해서 사용되는 경우에, 서비스 제공자들은 사용자에게 피싱 메시지로부터 적절한 보호를 제공하지 못한다. 즉, 클라이언트-측 애플리케이션의 대부분의 요소들이 서비스 제공자들에 의해 직접 제어되지 않기 때문에, 서비스 제공자는 사용자에게 피싱 이메일을 통보하는 일반적인 기술들의 구현을 제지당한다.

[0003] 본 기술들은 사용자에게 피싱 메시지들에 대한 적절한 보호 방안을 제공하도록 설정되지 않았다. 그런 이유로, 클라이언트-측 애플리케이션, 또는 비-웹 메일 클라이언트(non-web mail client)로부터 보는 경우에 피싱 메시지가 초래할 수 있는 잠재적 피해를 제한하는 방법을 적용하는 것은 사용자의 계정 내 메시지들을 보거나 그에 대해 행동을 취할 때 사용자의 경험을 개선할 수 있다.

발명의 내용

과제의 해결 수단

[0004] 이 요약은 상세한 설명에서 자세하게 후술 될 개념들을 개략적인 형태로 소개하기 위해 제공된다. 이 요약은 청구되는 기술의 핵심 특징 또는 키가 되는 특징들을 식별하기 위한 의도가 아닐 뿐만 아니라 청구되는 기술 범위의 영역을 제한하기 위한 의도 역시 가지지 않는다.

[0005] 본 발명의 실시예들은 일반적으로 디지털 메시지들(예를 들면 이메일 메시지, 인스턴트 메시지, 등)이 잠재적 피싱 이메일들로 식별된 때에 디지털 메시지들의 처리를 관리하는 컴퓨터화된 방법들과 컴퓨터 판독 가능 매체와 관련된다. 예시적 실시예에서, 서비스 제공자는 디지털 메시지들의 의도된 수신자에 배정된 계정의 거동을 제어하는데 이용된다. 계정 거동의 제어는 다양한 작업들을 포함할 수 있다. 그러나 각각의 이들 작업은 비-웹 메일 서버의 맥락에서 구현될 수 있다. 즉, 의도된 수신자는 비-웹 메일 서버에 의해 렌더링된 사용자 인터페이스(UI) 디스플레이를 통해서 사용자의 계정에 접속한다. 일반적으로, 비-웹 메일 클라이언트는 서비스 제공자로 하여금 UI 디스플레이의 측면들을 조정할 수 있게 하는 확장 프로토콜이 부족하기 때문에, 서비스 제공자는 UI 디스플레이의 설정을 제어 또는 조정할 수 없다. 그래서, 잠재적 피싱 이메일들로 식별된 디지털 메시지의 의도된 수신자에게 경고하는 일반적인 기술들은 효과가 없다.

[0006] 한 예시에서, 계정의 거동을 제어하는 작업은 잠재적 피싱 이메일로 식별된 디지털 메시지들에 메타데이터 태그를 첨부하는 단계와 그들을 정당한 이메일들(legitimate emails)로 식별된 디지털 메시지들로부터 격리된 태그된 디지털 통신물들(tagged digital communications)의 유지에 전담하는 저장 공간 내에 합치는 단계를 포함한다. 이 전담 저장 장소는 UI 디스플레이 상의 폴더에 맵핑되고, 표시될 수 있다. 폴더의 선택 직후에, 전담 저장 장소에 할당된 태그된 디지털 통신물들의 표현들(예를 들면 콘텐츠의 메타데이터와 디지털 통신물 속성들)이 수신자에게 포스트 된다. 그래서, 수신자는 직접 UI 디스플레이의 조정 없이도 태그된 디지털 통신물들의 위험한 상태에 대하여 경고를 받는다.

[0007] 더 나아가, 태그된 디지털 통신물들의 표현들을 향한 사용자-개시 행동들은 제한될 수 있다. 예를 들면, 사전에 제한되는 것으로 판단된 행동들(예를 들면 태그된 디지털 통신물의 이동 시도 명령, 응답 명령, 모두에 응답 명령, 전달 명령)을 일으키는 수신자의 요청은 수신자의 보안을 보호하기 위해서 서비스 제공자에 의해 실패된다. 예시로서, 행동의 실패는 요청을 가로채는 단계, 그 행동이 제한된 행동으로 분류되었는지를 확인하는 단계, 행동 대항인 디지털 통신물이 잠재적 피싱 이메일로 태그 되었음을 확인하는 단계, 행동의 구현을 실패시키

는 단계를 포함할 수 있다. 행동의 실패 직후에, 작업-실패 표시(즉 공지의 에러 코드)가 비-웹 메일 클라이언트에게 전송되고, 그 뒤에 행동이 서비스 제공자에 의해 수행되지 않았음이 수신자에게 통지된다. 그래서, 수신자는 태그된 디지털 통신물의 위험한 상태에 대하여 상기된다. 더 나아가, 비-웹 메일 클라이언트가 안티피싱 기능들을 지원하지 않음에도 불구하고, 이들 보안 조치들은 다른 사용자들에게 피해를 줄 수 있는 태그된 디지털 통신물의 분산에 대한 보호층을 제공한다.

[0008] 다른 실시예에서, 계정의 거동의 제어 작업은 잠재적 피싱 이메일들로 식별된 디지털 통신물들을 경고 메시지들로 대체하는 단계를 포함한다. 한 예시에서, 경고 메시지는 식별된 디지털 통신물이 잠재적 피싱 이메일일 수 있다는 통지를 전달한다. 다른 예시에서, 경고 메시지는 웹브라우저를 통해서 식별된 디지털 통신물의 콘텐츠를 접속할 수 있는 지침을 제공한다. 또 다른 예시에서, 경고 메시지는 사용자에 의해 선택될 때 사용자로 하여금 서비스 제공자에서 식별된 디지털 통신물의 콘텐츠에 대한 접속을 허용해주는 웹 브라우저로의 URL 링크를 포함한다. 그래서, 경고 메시지를 수신자에게 제공하고 식별된 디지털 통신물의 콘텐츠의 공개를 차단함으로써, 수신자는 디지털 통신물의 위험한 상태에 대하여 통지를 받고 무심코 위험한 웹사이트를 탐색하는 것으로부터 통제된다.

도면의 간단한 설명

[0009] 본 발명은 첨부된 도면들을 참조해서 아래에서 상세하게 서술된다.

도 1은 본 발명의 실시예들의 구현의 사용에 적절한 예시적 컴퓨팅 환경의 블록도이다.

도 2는 비-웹 메일 클라이언트의 맥락에서 잠재적 피싱 이메일들을 관리하도록 설정된, 본 발명의 실시예들의 구현의 사용에 적절한 분산 컴퓨팅 환경을 도시하는 블록도이다.

도 3은 본 발명의 한 실시예의 잠재적 피싱 이메일들의 식별 및 정리하는 기술에 대한 고 수준의 개요를 도시하는 운용상의 플로우 다이어그램이다.

도 4는 본 발명의 실시예에 따라서, 비-웹 이메일 클라이언트를 통해서 사용자게 계정에 접속할 때 사용자에게 잠재적 피싱 이메일을 경고하는 종합적인 방법을 도시하는 플로우 다이어그램이다.

도 5는 본 발명의 실시예에 따라서, 비-웹 메일 클라이언트를 통해서 접속한 때에 하나 이상의 디지털 통신물들의 처리를 관리하는 종합적 방법을 도시하는 플로우 다이어그램이다.

도 6은 잠재적 피싱 이메일들의 유지를 전담하는 저장 장소에 맵핑된 폴더를 나타내는 예시적 사용자 인터페이스의 도해적 스크린 디스플레이이다.

도 7은 잠재적 피싱 이메일의 콘텐츠를 공개하는 대신에 렌더링되는 경고 메시지를 나타내는 예시적 사용자 인터페이스의 도해적 스크린 디스플레이이다.

발명을 실시하기 위한 구체적인 내용

[0010] 본 발명은 여기서 법적 요건들을 충족시키기 위해서 특이성을 가지고 서술된다. 그러나 서술 그 자체는 본 발명의 범위를 제한하는 의도가 아니다. 오히려, 발명자들은 본 명세서에서 다른 현재 또는 미래 기술들과 함께 본 명세서에서 서술된 것과 다른 단계들 또는 유사한 단계들의 조합을 포함할 수 있도록 청구된 발명이 다른 방식으로도 구현될 수 있음을 고려한다.

[0011] 그래서, 한 실시예에서, 본 발명은 사용자가 비-웹 이메일 클라이언트를 통해서 계정을 접속할 때 잠재적 피싱 이메일을 사용자에게 경고하는 방법을 수행하는 하나 이상의 컴퓨터 판독 가능 매체에 구현된 컴퓨터 실행 가능 명령들과 관련된다. 처음에, 방법은 사용자와 연관된 계정에서 디지털 통신물을 수신하는 단계를 포함한다. 디지털 통신물을 잠재적 피싱 이메일로 식별하는 사건에 있어서, 메타데이터 태그(metadata tag)가 디지털 통신물에 첨부된다. 다음으로, 태그된 디지털 통신물은 잠재적 피싱 이메일들로 식별된 디지털 통신물들의 지속을 전담하는 저장 장소 내 위치하거나 또는 그와 연관된다. 저장 장소의 가상 표현은 사용자가 비-웹 이메일 클라이언트를 통해서 계정에 접속할 때 사용자에게 제시된다. 실시예들에서, 가상 표현은 잠재적 피싱 이메일들이 사용자의 계정에 도착했고 위험한 상태를 가지는 것으로 식별되었음을 사용자에게 나타내는 표시를 제공한다.

[0012] 다른 실시예에서, 본 발명의 측면들은 비-웹 메일 클라이언트를 통해서 접속될 때 하나 이상의 디지털 통신물들의 처리를 관리하기 위해 서버에서 구현되는 컴퓨터화된 방법을 포함한다. 방법은 디지털 통신물의 의도된 수

신자와 연관된 계정에서의 디지털 통신물의 수신을 감지하는 단계, 그리고 디지털 통신물을 수신한 직후, 디지털 통신물이 정당한 메시지(legitimate message)인지 아닌지 여부를 판단하기 위해서 필터링 휴리스틱(heuristics)을 적용하는 단계를 포함한다. 디지털 통신물이 부적절한 메시지(uninvited message)로 판단되는 경우, 디지털 통신물은 위험한 것으로 표시된다. 위험한 디지털 통신물은 위험한 디지털 통신물의 사용자-개시 접속 요청(user-initiated request)의 수신 직후에 경고 메시지로 대체된다. 실시예들에서, 경고 메시지는 다음 서비스들, 즉, 위험한 디지털 통신물이 잠재적 피싱 이메일로 식별되었다는 통지의 전달; 웹브라우저를 통해서 위험한 디지털 통신물의 콘텐츠의 접속 주의 사항 제공; 또는 선택시에 수신자에게 위험한 디지털 통신물의 콘텐츠 접속을 허용하는 URL(uniform-resource locator) 링크를 웹브라우저에 제공 중 적어도 하나를 수행하도록 기능할 수 있다.

[0013] 결국, 비-웹 메일 클라이언트는 사용자 인터페이스(UI) 디스플레이 내 렌더링되는 목록 내 위험한 디지털 통신물 표현을 표면화하도록 지시받는다. 일반적으로, 목록은 정당한 메시지들로 판단되는 디지털 통신물의 하나 이상의 표시들을 포함한다. 한 예시에서, 비-웹 메일 클라이언트에 의해 렌더링된 UI 디스플레이는 사용자 계정을 관리하는 서비스 제공자에 의해서 변경될 수 없다. 위험한 디지털 통신물의 표시의 사용자-개시 선택의 수신 직후에, 수신자에게 경고 메시지를 표시하고 위험한 디지털 통신물의 콘텐츠의 표시를 보류하도록 하는 명령들이 비-웹 메일 클라이언트에게 전달된다.

[0014] 또 다른 실시예에서, 본 발명은 컴퓨터 실행 가능 명령들이 구현되는 하나 이상의 컴퓨터 판독 가능 매체들을 포함하고, 컴퓨터 실행 가능 명령들은 실행될 때 비-웹 메일 클라이언트에 의해 렌더링된 사용자 인터페이스(UI) 디스플레이를 통해서, 잠재적 피싱 이메일이 사용자 계정에 도착했음을 사용자에게 통보하는 방법을 수행한다. 예시적 실시예에서, 방법은 잠재적 피싱 이메일들로 식별된 하나 이상의 디지털 통신물들의 지속을 전담하는 저장 장소를 생성하는 단계를 포함한다. 비-웹 클라이언트는 UI 디스플레이 내에서 폴더를 렌더링하도록 지시된다. 일반적으로, 폴더는 전담된 저장 장소에 맵핑된다.

[0015] 한 예시에서, 비-웹 메일 클라이언트로 하여금 UI 디스플레이 내에서 폴더를 렌더링하도록 지시하는 단계는 비-웹 메일 클라이언트로 하여금 정당한 이메일들로 식별된 디지털 통신물을 유지하는 저장 장소들에 맵핑되는 다른 폴더들을 포함하는 목록 내에 폴더로 렌더링하도록 지시하는 방법을 포함한다. 그에 따라, 잠재적 피싱 이메일들은 정당한 이메일들로부터 시각적으로 구분된다.

[0016] 어느 시점에, 폴더를 접속하기 위해 사용자에 의해 구현되는 조짐이 감지된다. 감지 직후에, 비-웹 메일 클라이언트는 식별된 디지털 통신물의 표시들을 렌더링하도록 지시된다. 한 예시에서, 표시들은 식별된 디지털 통신물들의 콘텐츠와 관련된 메타데이터를 포함한다.

[0017] 방법은 더 나아가 식별된 디지털 통신물들로 인도되는 사용자에 의해서 개시된 행동을 수신하는 단계를 포함한다. 만약에 행동이 사전 정의된 제한된 행동으로 인식되면, 사용자-개시 행동은 실패한 것이다. 한 예시에서, 실패한 사용자 행동은 행동의 실행을 방지하는 단계를 포함한다. 추가적으로, 작업-실패 표시(예를 들면 표준 에러 코드)는 비-웹 메일 클라이언트에게 전송될 수 있고, 이때 작업-실패 표시는 행동 실패의 통보를 전달한다.

[0018] 일반적으로, 본 발명의 실시예들은 잠재적 피싱 이메일들의 처리를 관리하는 단계와 관련된다. 여기서 활용되는 바와 같이, 구문 "잠재적 피싱 이메일"은 한정적으로 해석되는 것으로 여겨지지 않으며 사용자에게 쓸모없는 임의의 통신을 포함할 수 있다. 예를 들면, 잠재적 피싱 이메일들은 스팸 통신, 정크 인스턴트 메시지들, 그리고 피싱 이메일들을 포함할 수 있다. 앞에서 서술된 바와 같이, 피싱 이메일들은 수신자의 개인 정보(예를 들면, 사용자 이름, 패스워드, 크레디트 카드 정보 등)의 공개를 부정하게 유도할 의도로 다양한 소스들로부터 의도되는 수신자의 계정으로 보내진다. 이 유인책(inducement)은 피싱 이메일들이 소스를 신뢰할 수 있는 엔티티로 표시하기 때문에 효과적이다. 그러한 것으로서, 의심하지 않는 수신자들은, 본래는 신중한 정보를 제공하도록 유혹된다. 종종, 피싱 이메일은 정당한 이메일 또는 인스턴트 메시지와 유사한 모습 및 느낌을 가지고 있고 사용자가 부정하게 민감한 정보(예를 들면 은행 계정 로그온, 사용자 식별 정보, 주민 등록 번호, 등)를 누설 요청을 받도록 하는 가짜 웹사이트(즉 은행의 패러디 웹사이트)의 탐색을 인도하는 역할을 수행한다. 다른 경우들에서, 피싱 이메일은 사용자로 하여금 개인 정보를 피싱 이메일의 소스 또는 다른 불법적인 엔티티에 보내도록 미끼를 놓는다.

[0019] 여기서는 잠재적 피싱 이메일들이 문구들 "부적절한 메시지(uninvited message)," "태그된 메시지," "위험한 디지털 통신물," 그리고 "피싱 이메일로" 지칭되지만 각각의 이들 문구들은 바로 앞에서 서술된 "잠재적 피싱 이메일들"의 통상적 개념을 나타내기 위해 고려되어야할 것이다.

[0020] 예시적 실시예에서, 본 발명은 비-웹 메일 클라이언트의 상황에서 잠재적 피싱 이메일들의 처리를 관리하는 단계에서 적용된다. 여기서 활용된 바와 같이, 구문 "비-웹 메일 클라이언트"는 한정적으로 해석돼서는 안 되고, 웹 브라우저처럼은 통제될 수 없는 최종 사용자 장치(end-user device)(예를 들면 휴대용 장치, 컴퓨터, PDA, 또는 임의의 다른 클라이언트 장치)에서 실행되는 임의의 프로그램 또는 애플리케이션을 폭넓게 지칭할 수 있다. 즉, 비-웹 메일 클라이언트에 의해 제공되는 사용자 경험은 최종 사용자 장치로부터 먼 거리에 위치한 서버에서 실행되는 서비스 제공자(예를 들면 Hotmail)에 의해 제어될 수 없다. 예를 들면, 비-웹 메일 클라이언트에 의해 렌더링된 UI 디스플레이의 요소들은 서비스 제공자에서 수신된 메시지들을 기초로 해서 조정될 수 없다. 예를 들면, UI 디스플레이는 사용자에게 이메일 안의 피싱 콘텐츠를 경고하기 위해서, 사용자가 특정 통신에 대하여 취할 수 있는 행동들을 제한하기 위해서, 또는 사용자에게 잠재적 부적절한 메시지를 통지하기 위해서 다이내믹하게 변경될 수 없다.

[0021] 비-웹 매일 클라이언트에 대한 제어의 결여는 부분적으로는 다음 요소들 중 하나 이상의 요소들에 기인한다. 즉, 서비스 제공자 접속에 사용되는 기저 프로토콜이 디지털 통신물(즉, 메일 메시지)을 잠재적 피싱 이메일로 표시할 의미론을 가지고 있지 않는 다는 것; 비-웹 메일 클라이언트에 의해 렌더링된 UI 디스플레이가 서비스 제공자에 의해 조종되지 못한 다는 것(UI 디스플레이가 사용자 계정을 관리하는 서비스 제공자에 의해 변경될 수 없다); 그리고 비-웹 메일 클라이언트에게 클라이언트로 하여금 안티피싱(antiphishing) 경고와 같은 새로운 기능을 지원할 수 있게 해주는 확장 프로토콜이 없다는 것이다. 그런 이유로, 비-웹 메일 클라이언트(예컨대, Thunderbird)의 UI 디스플레이는 사전 결정되고 있고 서비스 제공자의 의사에 따라 다이내믹하게 관리될 수 없기 때문에, 사용자에게 잠재적 피싱 이메일들을 경고하고 그들로부터 사용자를 보호하는 일반적 기술들(예컨대, 인박스(inbox)의 UI 디스플레이를 변경하고, 특화된 툴박스를 제공하는 것)이 이용가능하지 않다.

[0022] 본 발명의 실시예들의 개요 및 특징들의 일부를 간략하게 서술한바, 본 발명의 구현에 적합한 예시적 운용 환경이 아래에서 서술된다.

[0023] 일반 도면들, 그리고 처음에는 특히 도 1을 참조하면, 본 발명의 실시예들의 구현을 위한 예시적 운용 환경이 일반적으로 컴퓨팅 장치(100)로 도시되고 지정된다. 컴퓨팅 장치(100)는 적합한 컴퓨팅 환경의 한 예시에 불과할 뿐, 발명의 기능 또는 사용의 범위를 제한하는 의도를 가지지 않는다. 또한, 컴퓨팅 장치(100)가 도시된 요소들의 임의의 하나 또는 그들의 조합과 관련해서 임의의 의존성 또는 필수 요건을 가지는 것으로 해석되어서도 안 될 것이다.

[0024] 발명은 컴퓨터 또는 개인용 데이터 보조기 또는 다른 휴대용 장치와 같은 다른 장치에 의해 실행되는 프로그램 요소들과 같은 컴퓨터 실행 가능 명령들을 포함하는 컴퓨터 코드 또는 장치-사용 가능 명령들(machine-useable instructions)의 일반적 맥락에서 서술될 수 있다. 일반적으로, 루틴들, 프로그램들, 객체들, 요소들, 데이터 구조들 등을 포함하는 프로그램 요소들은 특정 작업들을 수행하거나 또는 특정 압축 데이터 형식들을 구현하는 코드와 관련된다. 본 발명의 실시예들은 휴대용 장치들, 가전 제품들, 일반-목적 컴퓨터들, 전문 컴퓨팅 장치 등을 포함하는 다양한 시스템 설정들에서 실행될 수 있다. 발명의 실시예들은 또한 작업들이 통신 네트워크를 통해서 연결된 원격 처리 장치들에 의해 수행되는 분산 컴퓨팅 환경 내에서도 실행될 수 있다.

[0025] 계속해서 도 1을 참조하면, 컴퓨팅 장치(100)는 다음 장치들 즉, 메모리(112), 하나 이상의 프로세서들(114), 하나 이상의 표시 요소들(116), 입력/출력(I/O) 포트들(118), I/O 요소들(120), 그리고 구체적 전력 공급원(122)과 직접 또는 간접적으로 결합시키는 버스(110)를 포함한다. 버스(110)는 하나 이상의 버스들(어드레스 버스, 데이터 버스 또는 그들의 결합)을 나타낼 수 있다. 비록 도 1의 다양한 블록들이 명확성 차원에서 선들과 함께 도시되지만, 실제 현실에서는, 다양한 요소들을 설명하는 것은 명확하지 않고, 은유적으로, 선들은 보다 정확하게는 불분명하다. 예를 들면, 어떤 사람은 디스플레이 장치와 같은 표시 요소를 I/O 요소라고 생각할 수 있다. 또한, 프로세서들은 메모리를 가진다. 여기서 발명자들은 이러한 것이 당해 분야에서는 당연한 것임을 인지하고 도 1의 다이어그램은 본 발명의 하나 이상의 실시예들과의 관계에서 사용될 수 있는 단순한 예시적 컴퓨팅 장치라는 것을 강조한다. "워크스테이션," "서버," "랩톱," "휴대용 장치," 등과 같은 분류들 사이에서 차이는 두지 않고, 모든 것은 도 1의 범위 안에서 고려되고 "컴퓨터" 또는 "컴퓨팅 장치"에 관련된다.

[0026] 컴퓨팅 장치(100)는 일반적으로 다양한 컴퓨터 판독 가능 매체를 포함한다. 한정이 아닌 예시로써, 컴퓨터 판독 가능 매체는 RAM(random access memory); ROM(read only memory); EEPROM(electronically erasable programmable read only memory); CDROM, DVDs 또는 다른 광학 또는 홀로그래피 매체, 자기 카세트, 자기 테이프, 자기 디스크 저장부 또는 다른 자가 저장 장치들; 또는 원하는 정보를 인코드하는데 사용되고 컴퓨팅 장치(100)에 의해 접속될 수 있는 임의의 다른 매체를 포함할 수 있다.

[0027] 메모리(112)는 휘발성 및/또는 비휘발성 형태의 컴퓨터 저장 매체를 포함한다. 메모리는 이동식, 고정식, 또는 그들의 조합일 수 있다. 예시적 하드웨어 장치들은 고체-상태 메모리, 하드 드라이브들, 광학-디스크 드라이브들을 포함한다. 컴퓨팅 장치(100)는 메모리(112) 또는 I/O 요소들(120)과 같은 다양한 엔티티들로부터 데이터를 판독할 수 있는 하나 이상의 프로세서들을 포함한다. 표시 요소(들)(116)는 사용자 또는 다른 장치에게 데이터 징후들을 표시한다. 예시적 표시 요소들은 디스플레이 장치, 스피커, 프린팅 요소, 진동 요소 등을 포함한다. I/O 포트들(118)은 컴퓨팅 장치(100)로 하여금 I/O 요소들(120)을 포함하는 다른 장치들과 논리적으로 결합하도록 할 수 있고, 이 중 일부는 내장형일 수 있다. 출력 요소들은 마이크로폰, 조이스틱, 게임 패드, 위성 접시, 스캐너, 프린터, 무선 장치 등을 포함한다.

[0028] 일부 실시예들에서, 도 1의 컴퓨팅 장치(100)는 본 발명의 다양한 측면들을 구현하도록 설정된다. 한 예시에서, 이들 측면들은 잠재적 피싱 이메일들을 보기 위한 사용자-개시 요청의 감지 직후 또는 잠재적 피싱 이메일들에서 지시된 행동의 수신 직후에 잠재적 피싱 이메일들의 처리의 관리와 관련된다. 다른 예시에서, 이들 측면들은 잠재적 피싱 이메일들을 정당하다고 식별된 이메일들로부터 분리하는 단계와 잠재적 피싱 이메일들을 비-웹 메일 클라이언트의 사용자들에게 그들의 위험한 상태를 통지하는 방식으로 표시하는 단계와 관련된다.

[0029] 사용자에게 디지털 통신물이 위험하다는 것을 통지하는 것과 잠재적 피싱 이메일 때문에 개인 정보를 누설하는 것으로부터 사용자들을 보호하는 것이 이제 도 2를 참조해서 논의된다. 특히, 도 2는 본 발명의 실시예들 구현의 사용에 적합한 분산 컴퓨팅 환경의 예시적 시스템 아키텍처(200)를 도시한다. 일반적으로, 본 발명의 실시예들의 구현은 잠재적 피싱 이메일로 식별된 디지털 통신물의 의도된 수신자에게 통지하여 그 디지털 통신물이 위험한 상태로 표시되고, 그 디지털 통신물에 대하여 취할 수 있는 행동들(예를 들면 콘텐츠 보기, 다른 폴더로 이동, 답장 또는 전달 등)을 제한하는 것과 관련된다. 도 2에서 도시된 예시적 시스템 아키텍처(200)는 단지 하나의 적절한 컴퓨팅 환경의 예시에 불과하고 본 발명의 기능 또는 사용의 범위에 대한 임의의 제한을 제안하는 의도는 가지지 않는다. 또한, 예시적 시스템 아키텍처(200)가 도시된 임의의 단일 요소 또는 요소들의 결합과 관련해서 임의의 의존성 또는 필수 요건들을 가지는 것으로 해석되어서도 안 된다.

[0030] 처음에, 예시적 시스템 아키텍처(200)는 소스(210), 사용자(250), 클라이언트 장치(260), 데이터 저장부들(230)(즉 구조화된 검색 가능 데이터베이스들), 웹 서버(220) 그리고 이들 아이템들 각각을 상호 연결하는 네트워크(205)를 포함한다. 도 2에 도시된 클라이언트 장치(260), 데이터 저장부들(230) 그리고 웹 서버(220) 각각은 예를 들면 도 1을 참조하여 상술된 컴퓨팅 장치(100)와 같은 다양한 종류의 컴퓨팅 장치들의 형식을 가질 수 있다. 한정이 아닌 예시로써, 클라이언트 장치(260) 및/또는 웹 서버(220)는 개인용 컴퓨터, 데스크톱 컴퓨터, 랩톱 컴퓨터, 가전 제품, 휴대용 장치(예를 들면 PDA), 다양한 서버들, 프로세싱 장비 등일 수 있다. 그러나 본 발명은 이들 컴퓨팅 장치들에서 구현되는 것에 한정되지 않고 본 발명의 실시예들의 범위 안의 임의의 다양한 다른 종류들의 컴퓨팅 장치들 상에도 구현될 수 있음을 유의해야 한다.

[0031] 일반적으로, 각각의 장치들(260 및 220)은 컴퓨팅 유닛에서 실행되는 요소(들)의 작업들(예를 들면 수신 요소(221), 관리 요소(222), 저장 요소(223) 등)을 지원하기 위해서 어떤 형태의 컴퓨팅 유닛을 포함하거나 또는 그와 연결되어 있다. 여기서 활용되는 바와 같이, 구문 "컴퓨팅 유닛"은 일반적으로 소프트웨어, 애플리케이션, 그리고 컴퓨터 프로그램들의 실행에 기반이 되는 운용 시스템을 지원하는 프로세싱 파워 및 저장 메모리를 가지는 전용 컴퓨팅 장치를 나타낸다. 한 예시에서, 컴퓨팅 유닛은 각각의 장치로 하여금 통신-관련 프로세스들 및 다른 작업들(예를 들면 수신 요소(221)에서 디지털 통신물의 감지 그리고 관리 요소(222)에서 디지털 통신물을 잠재적 피싱 이메일로 식별)을 수행할 수 있게 하기 위해 장치(260 및 220)에 필수적, 또는 작업적으로 결합된 유형의 하드웨어 요소들, 또는 장치들로 구성된다. 다른 예시에서, 컴퓨팅 유닛은 각각의 장치들(260 및 220)을 동반하는 컴퓨터 판독 가능 매체에 결합된 프로세서(미도시)를 포함할 수 있다.

[0032] 일반적으로, 컴퓨터 판독 가능 매체는 프로세서에 의해 실행 가능한 복수의 컴퓨터 소프트웨어 요소들을 적어도 일시적으로 저장하는 물리적 메모리를 포함한다. 여기서 활용되는 바와 같이, 용어 "프로세서"는 한정적 의미가 아니고 컴퓨터의 수용력(capacity) 안에서 기능하는 컴퓨팅 유닛의 임의의 요소들을 포함할 수 있다. 이런 수용력에서, 프로세서는 명령들을 처리하는 유형의 물건으로 설정될 수 있다. 예시적 실시예에서, 프로세싱은 펫칭(fetching), 디코딩/해석, 실행, 후기입 명령들을 포함할 수 있다.

[0033] 또한, 명령들의 프로세싱에 더해서, 프로세서는 장치들(260 및 220)에 필수적 또는 그 위에 위치하는 다른 리소스에게 정보를 송수신할 수 있다. 일반적으로, 리소스들은 장치들(260 및 220)로 하여금 특정 기능의 수행을 가능하게 하는 소프트웨어 요소들 또는 하드웨어 메커니즘들과 관련 있다. 단지 예시로써, 웹 서버(220)에 의해 수용되는 리소스들은 수신 요소(221), 관리 요소(222), 저장 요소(223), 그리고 평가 요소(224) 중 하나 이

상을 포함한다. 이들 요소 중 하나 이상이 서비스 제공자(미도시)에게 특정 기능적 측면들을 제공하기 위해서 결합될 수 있다. 일반적으로, 서비스 제공자(예를 들면 Hotmail)는 메일 메시지들의 수신, 발신, 관리, 그리고 저장과 같은 사용자 온라인 계정(예를 들면 이메일 계정)의 측면들을 관리한다.

[0034] 다른 예시에서, 클라이언트 장치(260)에 의해 수용된 리소스들은 맵핑 요소(241), 렌더링 요소(242), 그리고 상호 작용 요소(243) 중 하나 이상을 포함할 수 있다. 이들 요소들 중 하나 이상은 비-웹 이메일 클라이언트(240)에게 특정 기능 측면들을 제공하기 위해서 결합될 수 있다. 일반적으로, 비-웹 이메일 클라이언트(예를 들면 Thunderbird)는 사용자로 하여금 서비스 제공자에 의해 지원되는 온라인 계정의 접속 및 관리를 허용하는 UI 디스플레이를 렌더링한다.

[0035] 클라이언트 장치(260)는 입력 장치(미도시)와 표시 장치(미도시)를 포함할 수 있다. 일반적으로, 여러 가지 중에서 사용자의 계정에서 지속되는 하나 이상의 디지털 통신물(215)에 대한 행동들은 물론이고 디지털 통신물(215)과 그것의 표현을 포함하는 폴더들의 표시에 영향을 미치는 입력(들)을 수신하도록 입력 장치가 제공된다. 출력 장치들은 마우스, 조이스틱, 키 패드, 마이크로폰, 도 1의 I/O 요소들(120), 또는 사용자의 입력을 수신할 수 있고 그 입력의 표시를 클라이언트 장치(260)에 전달할 수 있는 임의의 다른 요소를 포함한다.

[0036] 실시예들에서, 표시 장치는 그것에 대해 UI 디스플레이를 렌더링 및/또는 표시하도록 설정된다. 클라이언트 장치(260)의 출력에 작업적으로 결합된 표시 장치는 디지털 모니터, 전자 디스플레이 패널, 터치 스크린, 아날로그 셋 톱 박스, 플라스마 스크린, 오디오 스피커들, Braille 패드, 등과 같은 사용자에게 정보를 표시할 수 있는 임의의 표시 요소로 설정될 수 있다. 한 예시적 실시예에서, 표시 장치는 디지털 통신물 및 폴더들의 표현으로 가득 찬 디스플레이 영역과 같은 풍부한 콘텐츠를 표시하도록 설정된다. 다른 예시적 실시예에서, 표시 장치는 정당하다고 식별된 디지털 통신물과 연관된 콘텐츠의 렌더링할 수 있고, 또는 잠재적 피싱 이메일들로 식별된 디지털 통신물과 연관된 경고 메시지를 렌더링할 수 있다. 또 다른 예시적 실시예에서, 표시 장치는 미디어의 다른 형식들(예를 들면 오디오 신호), 또는 활성화(예를 들면 웹 사이트 탐색을 위해 사용자의 의해 선택될 수 있는) 또는 비활성화된 URL 링크들을 표시할 수 있다.

[0037] 데이터 저장부들(230)은 일반적으로 잠재적 피싱 이메일(들)로 식별된 디지털 통신물(들)에 첨부된 지속적인 태그들과 연관된 정보를 저장하도록 설정된다. 다른 경우들에서, 데이터 저장부들(230)은 데이터 저장부(230)에 의해 수용된 컴퓨터 판독 가능 매체 상의 격리 목록을 저장하도록 설정된다. 일반적으로, 격리 목록은 사용자 계정에 도착한 잠재적 피싱 이메일로 식별된 각각의 디지털 통신물들을 열거하는 인덱스로 기능한다. 다른 실시예에서, 격리 목록은 위험한 상태(예를 들면 스파이웨어, 스팸, 피싱 메시지들, 감염된 이메일들, 등)를 가지는 것으로 표시된 이메일 ID들의 명단을 포함한다.

[0038] 다양한 실시예들에서, 데이터 저장부들(230)에 저장된 정보는 한정 없이, 잠재적 피싱 이메일 콘텐츠 대신에 렌더링되는 경고 메시지들, 사용자 계정에서 수신된 디지털 통신물의 콘텐츠, 디지털 통신물의 위험 여부를 판단하는 필터링 휴리스틱(heuristics), 제한된 행동들의 목록, 그리고 여기서 논의된 바와 같이 서비스 제공자의 작업을 지원하는 임의의 다른 데이터를 포함할 수 있다. 추가적으로, 데이터 저장부들(230)은 저장된 정보의 적절한 접속에 대해 검색 가능하도록 설정된다. 예를 들면, 데이터 저장부(230)는 지속되는 잠재적 피싱 이메일들에 전담된 저장 장소와 연관된 디지털 통신물에 대해 검색 가능할 수 있다.

[0039] 본 기술 영역의 당업자들은 데이터 저장부(230) 내에 저장된 정보가 설정 가능하고 제한된 행동들과 전담 저장 장소의 생성 및 유지에 관련 있는 임의의 정보를 포함할 수 있다. 이런 정보의 콘텐츠와 용량은 어떤 식으로도 본 발명의 실시예들의 범위를 제한하는 의도를 가지지 않는다. 더 나아가, 단일, 독립 요소들로 도시되어있지만, 데이터 저장부들(230)은, 사실, 복수의 데이터베이스들일 수 있고, 예를 들면 그 일부가 클라이언트 장치(260) 상에 위치하는 데이터베이스 클러스터, 웹 서버(220), 다른 외장 컴퓨팅 장치(미도시), 및/또는 이들의 임의의 조합일 수 있다.

[0040] 이 예시적 시스템 아키텍처(200)는 본 발명의 측면들을 수행하기 위해 구현될 수 있는 적절한 환경의 하나의 예시에 불과하고 발명의 사용 또는 기능 범위에 대하여 제한을 가하는 의도는 가지지 않는다. 또한, 도시된 예시적 시스템 아키텍처(200) 도시된 바와 같이 장치들(260 및 220), 데이터 저장부들(230), 그리고 요소들(221, 222, 223, 224, 241, 242, 243)중 임의의 하나 또는 그들의 조합과 관련해서 어떠한 의존성 또는 필수 요건도 가지는 것으로 해석되어서는 안 된다. 일부 실시예들에서, 하나 이상의 요소들(221, 222, 223, 224, 241, 242, 그리고 243)은 독립 장치로 구현될 수 있다. 다른 실시예들에서, 하나 이상의 요소들(221, 222, 223, 224, 241, 242, 그리고 243)은 웹 서버(220)와 직접적으로 통합될 수도 있고, 또는 웹 서버(220)를 형성하기 위해서 상호 연결되는 분산 노드들 상에 있을 수도 있다. 본 기술 영역의 당업자들은 요소들(221, 222, 223, 224,

241, 242, 그리고 243)(도 2 에서 도시)은 예시적일 뿐이고 한정적으로 해석되어서는 안 된다는 것을 이해해야 할 것이다.

[0041] 그래서, 많은 요소들이 본 발명의 실시예들의 범위 안에서 요구되는 기능을 달성하기 위해서 적용될 수 있다. 도 2 의 다양한 요소들이 명료하게 보이기 위해서 선들과 함께 도시되지만, 실제 현실에서 다양한 요소들을 기술하는 것은 명료하지 않고, 은유적으로, 선들은 보다 정확하게는 불분명하다. 더 나아가, 도 2 의 일부 요소들은 단일 블록들로 도시되어 있지만, 도시는 현실적 예시이고 제한적으로 해석되어서는 안 될 것이다(예를 들면 단지 하나의 저장 요소(243)가 도시되어 있지만, 더 많은 저장 요소들이 웹 서버(220) 상에 수용되고, 데이터 저장부들(230)에서 구현되고, 또는 클라이언트 장치(260)와 통신적으로 결합될 수 있다).

[0042] 더 나아가, 예시적 시스템 아키텍처의 장치들은 관련 분야에서 공지된 임의의 방법으로 상호 연결될 수 있다. 예를 들면, 웹 서버(220)와 클라이언트 장치(260)는 하나 이상의 네트워크들(205)을 통해서 서로 결합된 복수의 컴퓨팅 장치들을 포함하는 분산 컴퓨팅 환경을 통해서 사용 가능하게 결합될 수 있다. 실시예들에서, 네트워크(205)는 하나 이상의 LAN들 및/또는 WAN들을 포함할 수 있고 이에 한정되지는 않는다. 이런 네트워킹 환경들은 사무실, 기업용 컴퓨터 네트워크들, 인트라넷, 그리고 인터넷에서 흔하다. 그래서, 네트워크는 여기서 더 추가적으로 서술되지는 않는다.

[0043] 가동 중일 때, 요소들(221, 222, 223, 224, 241, 242, 그리고 243)은 적어도 소스(210)로부터의 디지털 통신물(215)을 잠재적 피싱 이메일로 식별하는 단계, 디지털 통신물(215)이 위험한 상황을 가진다는 것을 나타내는 태그(예를 들면 메타데이터)를 디지털 통신물(215)에 첨부하는 단계, 그리고 사용자(250)에게 통지하고 사용자를 보호하는 해결책을 구현하는 단계를 포함하는 프로세스를 수행하도록 설계된다. 이들 해결책들은 사용자(250)에게 잠재적 피싱 이메일의 존재를 경고하는 것과 잠재적 피싱 이메일에 관해 사용자(250)에 의해 요청되는 행동들을 제한하는 것을 포함한다. 실시예들에서, 소스(210)는 사용자의 개인 정보 공개를 부정하게 유도하는 메시지들(예를 들면 디지털 통신물(215))을 사용자(250)에게 전송하는 범죄 또는 불법 컴퓨터 프로그램들과 같은 하나 이상의 부정한 엔티티들을 표시한다. 실시예들에서, 사용자(250)는 소스(210)에 의해 분산되는 디지털 통신물(215)의 의도되는 수신자에 해당하는 임의의 엔티티를 나타낸다. 예시로써, 사용자(250)는 서비스 제공자에서의 계정과 연관되거나, 또는 비-웹 이메일 클라이언트(240)를 통해서 계정을 접속할 수 있는 클라이언트 장치(260)를 소유/점유하는 사람일 수 있다.

[0044] 처음에, 수신 요소(221)는 소스(210)로부터의 디지털 통신물(215)을 수신하고 감지하는 임무를 가진다. 수신 요소(221)는 그 뒤에 사용자(250)의 계정과 연관된 디지털 통신물(215)을 지속시키는 목적을 위해 데이터 저장부(230) 또는 웹 서버(220) 상에 수용된 저장 요소(223)로 디지털 통신물(215)을 전달한다. 디지털 통신물(215)의 저장을 용이하게 하는 것과 함께, 수신 요소(221)는 디지털 통신물(215)을 관리 요소(222)에 전달할 수 있다.

[0045] 디지털 통신물(215)의 수신 직후에, 관리 요소(222)는 다양한 작업들을 수행하도록 설정된다. 처음에, 작업들은 정당한 디지털 통신물으로부터 위험한 및/또는 부적절한 디지털 통신물들(215)을 필터링하는 단계를 포함한다. 한 예시에서, 필터링 작업은 디지털 통신물(215)이 잠재적 피싱 이메일인지 여부를 식별하고 그런 것들에 대하여 디지털 통신물(215)을 표시한다. 디지털 통신물(215)을 위험한 또는 정당한 것으로 식별하는 단계는 필터링 경험적 학습법을 적용하는 분석에 기초할 수 있다. 이들 필터링 경험적 학습법은, 도착하는 디지털 통신물(215)의 스캐닝 직후에, 디지털 통신물(215)이 신뢰성 있는 사이트 또는 위험한 이메일의 알려진 소스로부터 도착했는지 여부, 및/또는 디지털 통신물의 콘텐츠가 적대적 또는 위험 문지방 값을 만족하는지 여부를 판단한다.

[0046] 바로 앞에서 서술된 하나 이상의 기준들에 기초하여, 디지털 통신물(215)은 잠재적 피싱 이메일로 식별될 수 있고 위험한 상황을 가지는 것으로 표시될 수 있다. 필터링 경험적 학습법은 정밀하지 않고 가끔은 오류(이메일의 속성들에 기초하여 허위 양성을 제공)를 가지기 때문에, 디지털 통신물(215)가 정말 안전한지에 대한 최종적인 결정을 사용자(250)가 내릴 수 있도록 위험하다고 간주된 디지털 통신물(215)도 "잠재적" 피싱 이메일들로 고려되며, 이에 의해 이메일의 실제 성질을 확인할 수 있다. 이것은 메시지를 "피싱 이메일"로 식별하여 사용자에게 식별을 인증할 기회를 제공하지 않은 채 자동적으로 사용자의 계정으로부터 삭제하도록 하는 것과는 대조된다.

[0047] 실시예들에서, 디지털 통신물(215)을 잠재적 피싱 이메일 또는 위험한 상황을 가지는 것으로 표시하는 것은 디지털 통신물(215)에 태그를 첨부하는 것을 포함한다. 이 태그는 디지털 통신물(215)과 연관되어 저장되고 디지털 통신물(215)의 저장 장소 및 디지털 통신물(215)에 대하여 어떤 행동들이 제한되는지 여부를 관리하는데 사

용되는 메타데이터를 포함할 수 있다.

[0048] 디지털 통신물(215)을 위험한 또는 잠재적 피싱으로 표시하는 한가지 방법이 서술되었지만, 본 기술의 당업자들은 잠재적 피해를 표시할 수 있는 다른 종류의 적절한 표시 계획들이 사용될 수 있음과 본 발명의 실시예들이 여기서 서술된 첨부된 메타데이터 태그에 한정되지 않음을 이해해야할 것이다. 예를 들면, 위험한 디지털 통신물(215)은 사용자 계정에 도착한 각각의 잠재적 피싱 이메일들을 나열하는 격리 목록에 위험한 디지털 통신물(215)의 식별을 추가하는 방식으로 파악될 수 있다.

[0049] 다른 실시예들에서, 관리 요소(222)에 의해 수행되는 작업들은 디지털 통신물(215)이 잠재적 피싱 이메일이라는 것을 확인한 직후, 잠재적 피싱 이메일들로 식별된 디지털 통신물(215)을 지속하는데 전담되는 저장 장소를 생성하는 단계를 포함한다. 만약에 전담된 저장 장소가 이미 존재한다면, 위험(예를 들면 메타데이터 태그에 첨부된 메시지들) 하다고 표시된 디지털 통신물(215)은 전담 저장 장소에 배치되고, 또는 적어도, 전담 저장 장소와 관련되어 저장된다. 한 예시에서, 전담 저장 장소는 저장 요소(243)에 의해 관리되며 데이터 저장부들(230) 및/또는 웹 서버(220) 상의 메모리를 사용한다.

[0050] 일반적으로, 전담 저장 장소는 사용자 계정과 연관된 다른 디지털 통신물들(예를 들면 정당한 메시지로 식별된)이 지속되는 메모리 장소로부터 분리된 물리적 메모리 장소를 제공하도록 기능한다. 그런 이유로, 사용자가 비-웹 메일 서버(240)를 통해서 계정을 접속할 때, 맵핑 요소(241)는 분리된 저장 장소들을 감지하고 각각의 분리된 저장 장소에 맵핑되는 폴더들을 생성한다. 즉, 맵핑 요소(241)는 웹 서버(220)상의 저장 장소를 반영하기 위해서, UI 디스플레이 또는 클라이언트 시야 내의 폴더들을 정리하도록 설정된다. 예시로써, 정당한 메시지들을 보관하는 저장 장소와 맵핑되는 "인박스" 폴더가 만들어질 수 있고, 잠재적 피싱 이메일들로 식별된 디지털 통신물(215)을 보관하는 구별되는 "피싱 메일들" 폴더가 만들어질 수 있다. 이렇게 하여, 사용자(250)의 관심이 수신된 디지털 통신물들(215)의 코퍼스(corpus)로부터 특정 메시지들의 격리에 모아지고, 따라서 위험한 또는 잠재적 피싱 이메일들이 존재한다는 것을 사용자(250)에게 경고한다.

[0051] 폴더들의 생성과 적절한 디지털 통신물들(215)로 폴더들을 채운 직후에(저장 장소와 폴더들 사이의 맵핑에 기초하여), 렌더링 요소(242)는 UI 디스플레이에서 사용자에게 폴더들을 공개한다. 한 예시에서, 공개는 각각의 폴더의 타이들을 각각 포스팅하는 것을 포함할 수 있다. 예시로써, 정당한 메시지들을 보관하는 저장 장소에 맵핑된 폴더의 타이틀 "인박스"는 인박스 폴더의 디스플레이 옆에 위치할 수 있고, 전담 저장 장소에 맵핑된 폴더의 타이틀 "피싱 메일들"은 피싱 메일들 폴더 디스플레이 옆에 위치할 수 있다. 그런 이유로, 서비스 제공자는 사용자에게 그 특정 메시지는 위험한 것으로 간주된다는 것을 전달할 수 있고, 웹브라우저의 UI 디스플레이를 조정할 수 없는 경우 피싱 메일 폴더에서 지속되는 위험한 메시지들에 대한 사용자-개시 행동들이 왜 제한되는지를 전달할 수 있다. 즉, 피싱 메일 폴더를 표면화하는 것은 사용자에게 피싱 행동에 관해 통지 실패하는 것과 관련되는 비-웹 메일 클라이언트(240)의 문제의 완화 방안이고, 이때 완화책은 사용자(250)로 하여금 인박스 폴더의 맥락에서 피싱 메일 폴더를 볼 수 있게 해주는 것을 포함한다. 유리하게, 피싱 메일 폴더는 사용자(250)에게 폴더 탐색에 있어서 지속적이고 직관적인 경험을 제공하고, 비-웹 메일 클라이언트(240)의 한계 내에서 허용될 수 있다.

[0052] 앞에서 상세하게 설명된 바와 같이, UI 디스플레이는 비-웹 메일 클라이언트(240)가 실행 중인 클라이언트 장치(260)와 사용 가능하게 결합된 표시 장치에서 렌더링될 수 있다. 예를 들면, 도 6을 참조하면, 예시적 UI 디스플레이(600)는 인박스 폴더(620)의 표시가 피싱 메일 폴더(630)의 표시와 폴더 목록(640) 안에서 근접성을 가지는 것을 포함하도록 렌더링된다. 하나 이상의 폴더들(620 또는 630)의 선택 직후에, 각각의 폴더들(620 또는 630)에서 지속되는 디지털 통신물들(215)의 표시는 UI 디스플레이(600)에서 디스플레이된다. 이 실례에서 나타난 바와 같이, 인박스 폴더(620)가 선택되었다. 그와 같이, 인박스 폴더(620) 내에 저장된 디지털 통신물(215)의 일부의 표시가 인박스(680)에서 표시된다. 그런 이유로, 사용자(250)는 이들 디지털 통신물들(215)이 정당하다고 식별되었고 안전하게 읽거나, 저장하거나, 전송할 수 있음을 이해한다.

[0053] 일반적으로, 디지털 통신물(215)의 표현들은 디지털 통신물들(215)의 속성들 및/또는 콘텐츠로부터 얻어진다. 예를 들면, 디지털 통신물들(215)의 표현들은 도 6의 인박스(680) 내 메시지들(665 및 675)의 표시에 의해 도시된 바와 같이 콘텐츠의 스냅 샷, 날짜, 보낸 사람, 및/또는 디지털 통신물(215)의 타이틀 또는 제목란에 부합하는 헤더(header)를 포함할 수 있다. 디지털 통신물(215)의 표현의 선택(예를 들면 마우스 클릭) 직후에, 상호작용 요소(243)는 디지털 통신물(215)의 콘텐츠를 불러오는 명령을 서비스 제공자에게 전송한다. 그 후에 서비스 제공자는 디지털 통신물(215)이 위험한 상태로 표시되었는지 또는 잠재적 피싱 이메일로 식별되었는지 여부를 판단하기 위해서 디지털 표시에 첨부된 태그(들)를 조사한다. 만약에 잠재적 피싱 이메일 또는 위험한 것으

로 식별된 경우, 서비스 제공자는 렌더링을 위해서 선택된 디지털 통신물(215)의 콘텐츠를 비-웹 메일 클라이언트(240)에게 전달할지 또는 콘텐츠를 경고 메시지(도 7의 참조 번호 700 참고)로 대체할지 여부를 판단할 수 있다.

[0054] 하나의 해결 방안에서, 일반적으로 사용자-개시 선택이 잠재적 피싱 이메일(디지털 통신물(215)에 첨부된 메타데이터 태그에 의해 조사)로 표시된 디지털 통신물(215)의 표시로 향하는 것이 확인되고, 그리고 디지털 통신물(215)가 전담 저장 장소에서 유지되고 있음이 확인되면, 디지털 통신물(215)의 콘텐츠의 일부는 사용자(25)에 의해 검사되기 위해서 표면화된다. 이 해결책에서, 전담 저장 장소 내에서 유지되고 있는 잠재적 피싱 이메일의 콘텐츠 내에 포함된 하나 이상의 URL 링크들이 비활성화된다. 그래서, 사용자(250)는 콘텐츠의 조사에 의해 잠재적 피싱 이메일이 진짜 위험하거나 초대받지 않았는지 여부를 판단할 수 있으면서도, 잠재적 피싱 이메일을 통해 부정한 웹사이트를 탐색하는 것으로부터 보호될 수 있다. 유리하게, URL 링크를 사용 불가능하게 하는 것은 잠재적 위험 사이트(예를 들면 spoofed site)에 대한 사용자의 노출을 감소시키고 사이트 방문 시도에 의해 유발될 수 있는 금전적 및 개인적 손해를 효과적으로 경감한다.

[0055] 두 번째 해결책에서, 일반적으로 사용자-개시 선택이 잠재적 피싱 이메일로 표시된 디지털 통신물(215)을 향한다는 것이 확인되고, 그 디지털 통신물(215)이 정당한 통신(인박스 폴더에 맵핑된)을 포함하는 일반적 저장 장소에서 유지되고 있을 때, 선택된 디지털 통신물(215)의 콘텐츠는 사용자(250)에 의한 검사를 위해 표면화될 수 있는 경고 메시지로 대체될 수 있다. 이 해결책에서, 사용자에게 가능한 피해를 통지하기 위해서 전담 저장 장소를 사용하는 대신에, 경고 메시지는 선택된 디지털 통신물(215)이 위험한 상태를 가지는 것으로 고려된다는 것을 사용자에게 통지하는 기능을 수행한다. 선택된 디지털 통신물(215)의 콘텐츠가 공개되지 않기 때문에, 경고 메시지는 선택적으로 명령들 및/또는 선택시에 사용자로 하여금 웹브라우저를 탐색하게 하는 URL 링크를 포함할 수 있다. 웹 브라우저는 사용자(250)로 하여금 서비스 제공자에 의해 다이내믹하게 제어되는 보호되는 환경 안에서 선택된 디지털 통신물(215)의 콘텐츠를 볼 수 있게 해주고 사용자(250)가 선택된 디지털 통신물(215)과 상호 작용하는 동안에 경고들 및 다른 보안 조치들을 취할 수 있다. 그래서, 사용자(250)는 잠재적 피싱 이메일을 숨기는 방식에 의해 부정한 웹사이트의 탐색으로부터 실질적으로 보호되나, 그것이 실제로 위험하고 부적절한 것인지를 확인하기 위해서 여전히 웹브라우저에서 잠재적 피싱 이메일의 콘텐츠를 접속할 수 있다.

[0056] 예시적 실시예에서, 사용자(250)는 잠재적 피싱 이메일들로 식별된 하나 이상의 디지털 통신물들(215)에 대한 행동 수행을 시도할 수 있다. 한 예시에서, 사용자(250)는 위험하다고 표시된 디지털 통신물에 대하여 "이동" 행동의 부가 시도를 할 수 있다. 예시로써, 이동 행동은 위험한 디지털 통신물을 전담 저장 장소에서 정당하다고 식별된 디지털 통신물들을 보관하는 저장 장소로의 이동 시도를 포함한다. 실시예들에서, 이동 행동은 사용자(250)가 이동을 작동시키는 때와 근접한 시간 또는 비-웹 메일 클라이언트(240)와 서비스 제공자가 동기화될 때에 요청(270)으로 전송될 수 있다.

[0057] 이 이동 행동은 요청(270) 내에서 상호 작용 요소(243)를 통해서 서비스 제공자의 평가 요소(224)로 전송될 수 있다. 일반적으로, 평가 요소(224)는 사용자에 의해 개시된 요청(270)을 가로채고 이동 행동이 위험한 디지털 통신물을 목표로 하는지 여부를 판단한다. 만약에 그렇다면, 평가 요소(224)는 이동 행동이 제한된 행동의 목록에 해당하는지 여부를 판단한다. 만약에 그렇다면, 평가 요소(224)는 전담 저장 장소 밖으로 위험한 디지털 통신물을 이동하는 것을 허용하지 않는다. 그래서, 동기화 직후, 위험한 디지털 통신물의 표현은 피싱 메일 폴더로 돌아오고, 이는 전담 저장 장소에 맵핑되고, 그에 따라 사용자에게 그 디지털 통신물은 계속해서 위험한 상태로 간주된다는 것을 통지한다. 다시 말하면, 사용자(250)는 위험한 디지털 메시지들을 피싱 메일 폴더에서 임의의 다른 폴더로 이동시킬 수 없고 그 이동이 웹 서버(220)에 반영되게 할 수 없다. 이동 행동이 허용된 경우라 할지라도, 위험한 디지털 통신물을 전담 저장 장소로부터 나가게 하는 것은 메타데이터 태그 및 위험한 디지털 메시지와 연관된 관련 기능에 영향을 미치지 않는다.

[0058] 다른 예시에서, 사용자(250)는 위험하다고 표시된 디지털 통신물에 대하여 다른 제한된 행동을 시도할 수 있다. 예시로써, 이들 제한된 행동들은 하나 이상의 답신 명령, 모두에 대해 답신 명령, 그리고 전달 명령을 포함한다. 여러 가지 다른 명령들이 제한된 행동들로 서술되었지만, 본 기술 영역의 당업자들은 디지털 메시지들을 목표로 하는 사용자에 의해 취해진 다른 종류의 적절한 명령들도 제한된 행동들(예를 들면 저장 명령, 편집 명령, 등)로 고려될 수 있고, 본 발명의 실시예들은 여기서 서술된 이들 명령들로 한정되지 않음을 이해해야 할 것이다.

[0059] 위험한 디지털 통신물에 대한 제한된 행동의 관리시에, 제한된 행동은 요청(270) 안에서 상호 작용 요소(243)를 통해서 평가 요소(224)로 전송될 수 있다. 다시, 평가 요소(224)는 요청(270)을 가로채고 제한된 행동이 위험

한 디지털 통신물을 대상으로 하는지 여부를 판단한다. 예시로써, 위험한 또는 잠재적 피싱 디지털 통신물이 목표인지 여부를 판단하는 것은 선택된 디지털 통신물의 식별이 격리 목록에 나타나는지 여부를 확인하기 위해서 격리 목록을 체크하는 것을 포함한다. 다른 예시에서, 위험한 디지털 통신물이 목표인지 여부를 판단하는 것은 디지털 통신물을 피싱 메시지로 표시하는 태그가 디지털 통신물에 첨부되었는지 여부를 확인하기 위해서 선택된 디지털 통신물을 검사하는 것을 포함한다.

[0060] 일반적으로, 선택된 디지털 통신물에 첨부된 메타데이터 태그는 디지털 통신물이 어떻게 처리되는지와 요청(270)에서 제출된 행동이 존중되는지 여부를 관리한다. 추가적으로, 태그를 포함하는 메타데이터는 특정 행동은 허용하고 다른 것들은 불허하도록 조정될 수 있다. 그래서, 제한된 행동들은 각각의 디지털 메시지들과 연관된 위험도 판단과 위험도를 태그 안의 메타데이터 형태로 제출함에 있어서 필터링 휴리스틱상의 각각의 디지털 메시지에 대해 특정화될 수 있다.

[0061] 만약에 사용자(250)에 의해 위험한 디지털 통신물이 대상이 된다면, 평가 요소(224)는 행동 전부 또는 일부의 실행을 허용하지 않는다. 한 예시에서, 행동 실행의 실패는 명령으로 하여금 디지털 통신물(215)을 "답신" 또는 "전달"에 하는 것에 대한 실패를 포함한다. 더 나아가, 작업-실패 표시, 또는 공지의 에러 코드가 실패된 요청(270)에 대한 응답으로 비-웹 메일 클라이언트(240)에 보내진다. 한 예시에서, 작업-실패 표시는 제한된 행동의 실행 실패가 의도적인 이 경우와는 대조되는, 행동 수행시에 서비스 제공자가 실제 에러를 맞이할 때 생성되고 전송되는 것과 실질적으로 유사하다. 다른 예시에서, 작업-실패 표시를 전송하는 것은 그것 때문에 이미 알려진 에러 코드를 비-웹 메일 클라이언트(240)에게 돌려보내 주는 것을 포함한다. 이 경우에서, 비-웹 메일 클라이언트(240)는 사용자-관리 행동이 실패했음을 사용자(250)에게 자동으로 메시지, 시각적 표시(예를 들면 팝업 디스플레이), 또는 다른 표현으로 전달할 수 있다. 그래서, 실패 메시지 또는 표시가 사용자(250)에 의해 선택된 디지털 통신물이 잠재적 피싱 이메일로 식별된다는 것을 강화시킨다.

[0062] 추가적으로, 위험한 디지털 통신물들에게 집행될 수 있는 사용자의 행동들의 제한을 통해서, 서비스 제공자는 잠재적 피싱 이메일의 분산과 임팩트를 제어한다. 유리하게, 어떠한 안티피싱 기능도 지원하지 않는 웹-메일 클라이언트(240)의 범위 내에서 작동하는 앞에서 서술된 보안 조치들을 고려할 때, 사용자가 잠재적 피싱 메일에 대해 응답하는 것이 금지되므로 사용자 안전이 보장된다.

[0063] 이제 도 3으로 넘어가면, 본 발명의 한 실시예의 잠재적 피싱 이메일들의 식별 및 정리 기술의 고차적 개요(high level overview)를 도시하는 운용상 플로우 다이어그램(300)이 도시된다. 용어 "단계" 및/또는 "블록"은 여기서 적용되는 방법들의 다른 요소들을 함축하기 위해서 사용되지만, 용어들은 각각의 단계들의 순서가 명쾌하게 서술된 경우가 아니라면, 여기서 개시된 다양한 단계들 사이의 임의의 특정 순서를 의미하는 것으로 해석되어서는 안 된다.

[0064] 처음에, 플로우 다이어그램(300)은 여러 작업을 수행하는 서비스 제공자(310)를 보여준다. 서비스 제공자(310)는 도 2의 웹 서버(220) 또는 비-웹 메일 클라이언트(240)로부터 떨어져 있는 임의의 다른 하드웨어에 의해 지원될 수 있다. 서비스 제공자(310)에 의해 수행되는 작업들은 소스(210)(단계 315 참조)로부터 메시지(예를 들면 도 2 의 디지털 통신물(215))를 수신하는 단계 그리고 메시지가 잠재적 피싱 이메일인지 여부를 확인하는 단계(단계 320 참조)를 포함한다. 메시지가 잠재적 피싱 이메일로 확인되면, 서비스 제공자(310)는 단계 325에서 볼 수 있듯이, 메시지에 그 메시지가 잠재적 피싱 이메일이라는 것을 식별하는 메타데이터 태그를 첨부한다.

[0065] 앞에서 서술된 첫 번째 해결책을 참조하면, 태그된 메시지는 잠재적 피싱 이메일들을 지속하는데 전담된 저장 장소에 저장될 수 있고 비-웹 메일 클라이언트(240)에 의해 렌더링된 UI 디스플레이 상의 피싱 메일 폴더 안에서 사용자에게 표시될 수 있다. 앞에서 서술된 두 번째 해결책을 참조하면, 태그된 메시지는 정당한 메시지들과 함께 공동 저장 장소 안에 저장될 수 있고 비-웹 메일 클라이언트(240)에 의해 렌더링된 UI 디스플레이 상의 인박스 폴더 안에서 사용자(250)에게 표시될 수 있다. 그러나 태그된 메시지 표현의 사용자-개시 선택은 서비스 제공자로부터 태그된 메시지의 본래 콘텐츠를 대체하는 경고 메시지를 불러올 것이다.

[0066] 단계 330에서 도시된 바와 같이, 사용자(250)와 연관된 계정을 보기 위한 사용자-개시 명령은 비-웹 메일 클라이언트(240)에서 수신되고 서비스 제공자(310)에게 전달된다. 예시로써, 보기 명령(view command)은 사용자(250)가 계정에 로그인하고 계정을 활성화할 때 자동으로 보내질 수 있다. 보기 명령의 수신 직후에, 단계 340에서 도시된 바와 같이, 서비스 제공자(310)는 폴더들이 설정된 저장 장소들에 맵핑하도록 폴더들을 정리하고 태그된 메타데이터를 기초로 적절한 메시지들로 폴더들을 채운다. 정리된 폴더들은, 단계 350에서 도시된 바와 같이, 비-웹 메일 클라이언트(240)에 의해 렌더링되고 UI 디스플레이 상에 표시된다. 이들 정리된 폴더들은 각각의 폴더를 점유하는 메시지들에 첨부된 상태(안전 또는 위험)를 사용자(250)에게 알리는 기능을 수행한다.

[0067] 결국, 하나 이상의 메시지들에 대해 행동을 집행하는 요청(도 2의 요청(270)과 같은)이 사용자(250)로부터 수신된다. 이것은 단계 360에서 도시된다. 이 요청은 적어도 다음과 같은 두 가지 기준, 즉, 요청 대상인 메시지(들)에 첨부된 메타데이터가 메시지(들)가 잠재적 피싱 이메일로 식별된 것으로 나타내는지 여부; 그리고 집행된 행동이 제한된 행동인지 여부를 기초로 요청을 존중할지 여부를 판단하는 서비스 제공자(310)에게 보내진다. 만약 두 가지 조건중 하나도 충족되지 않는다면, 행동은 수행된다. 그렇지 않다면, 제한된 행동은 잠재적 피싱 이메일로 식별된 메시지(들)에서 구현되지 않는다. 이것은 단계 370에서 도시된다. 단계 380에서 도시된 바와 같이, 행동이 구현되지 않는 경우 또는 거절되는 경우에, 작업-실패 표시가 비-웹 메일 클라이언트(240)에게 보내진다.

[0068] 도 4를 참조하면, 본 발명의 실시예들에 따라, 비-웹 메일 클라이언트를 통해서 사용자가 계정에 접속할 때 사용자에게 잠재적 피싱 이메일을 경고하는 전체적인 방법(400)이 도시된다. 처음에, 방법(400)은 블록(410)에서 도시된 바와 같이, 사용자와 연관된 계정에서 디지털 통신물을 수신하는 단계를 포함한다. 디지털 통신물을 잠재적 피싱 이메일로 식별하고 나서, 블록 420에서 나타난 바와 같이, 메타데이터 태그가 디지털 통신물에 첨부된다. 그 다음에, 블록 430에서 나타난 바와 같이, 태그된 디지털 통신물이 잠재적 피싱 이메일들로 식별된 디지털 통신물들을 유지하도록 전담된 저장 장소 내에 위치, 또는 연관된다. 저장 장소의 시각적 표현은 블록 440에서 도시된 바와 같이, 비-웹 메일 클라이언트를 통해서 사용자가 계정을 접속할 때 사용자에게 표시된다. 실시예들에서, 시각적 표현은 사용자에게 잠재적 피싱 이메일들이 사용자 계정에 도착했고 위험한 상태로 식별되었었다는 표시를 제공한다.

[0069] 도 5를 참조하면, 본 발명의 실시예에 따라, 비-웹 메일 클라이언트를 통해서 접속된 하나 이상의 디지털 통신물들의 처리의 관리를 위한 종합적인 방법(500)을 나타내는 플로우 다이어그램이 도시된다. 처음에, 방법(500)은 디지털 통신물의 의도된 수신자와 연관된 계정에서 디지털 통신물의 수신을 감지하는 단계를 포함한다. 블록 510에서 도시된 바와 같이, 디지털 통신물의 수신 직후에, 디지털 통신물이 초대받지 못한 메시지인지 정당한 메시지인지 여부를 판단하기 위해서 펄터링 휴리스틱이 적용된다. 디지털 통신물이 초대받지 못한 메시지로 판단되는 경우에, 디지털 통신물은 블록 520에서 도시되는 바와 같이 위험한 것으로 표시된다. 블록 530에서 도시된 바와 같이, 위험한 디지털 통신물에 대한 사용자 개시 접속 요청 수신 직후에, 위험한 통신 메시지는 경고 메시지로 대체된다. 실시예들에서, 경고 메시지는 아래 서비스들, 즉, 위험한 디지털 통신물이 잠재적 피싱 이메일로 식별되었다는 통지의 전달; 웹 브라우저를 통해서 위험한 디지털 통신물의 콘텐츠를 접속하는 지침 제공; 또는 선택시에 수신자로 하여금 위험한 디지털 통신물의 콘텐츠를 접속하게 해주는 URL 링크를 웹브라우저에 제공 중 적어도 하나를 수행하도록 기능할 수 있다.

[0070] 결국, 블록 540에서 도시된 바와 같이, 비-웹 메일 클라이언트는 사용자 인터페이스(UI) 디스플레이 내에서 렌더링된 목록 내의 위험한 디지털 통신물의 표현을 나타내도록 지시된다. 일반적으로, 목록은 정당한 메시지들로 판단된 하나 이상의 디지털 통신물들의 표현들을 포함한다. 한 예시에서, 비-웹 메일 클라이언트에 의해 렌더링된 UI 디스플레이는 사용자 계정을 관리하는 서비스 제공자에 의해서 변경될 수 없다. 위험한 디지털 통신물의 표현의 사용자-개시 선택 수신 직후에, 수신자에게 경고 메시지를 표시하고 위험한 디지털 통신물의 콘텐츠의 공개를 보류하기 위해서 지시들이 비-웹 메일 클라이언트에게 전달된다. 이는 블록 550에서 도시된다.

[0071] 도 6을 참조하면, 잠재적 피싱 이메일을 지속하는데 전담된 저장 장소로 맵핑되는 폴더를 나타내는 예시적 사용자 인터페이스(600)의 도해적 스크린 디스플레이가 도시된다. 앞에서 논의된 바와 같이, 인박스 폴더(620)와 피싱 메일 폴더(630)가 폴더 목록(640) 내에서 디스플레이될 수 있다. 실시예들에서, 폴더들(620 및 630)의 구조는 서비스 제공자에서의 저장 장소들의 관리에 맵핑되고, 각각의 폴더들(620 및 630)에 포함된 메시지들은, 각각 분리된 저장 장소들(예를 들면 전담 그리고 공동)에 보관되는 메시지들에 맵핑된다.

[0072] 더 나아가, 메시지들(660)의 표현들은 사용자 인터페이스(600) 상에서 디스플레이된다. 한 실시예에서, 위험한 상태를 나타내는 메타데이터 태그가 첨부된 메시지들(660)의 표현들은 피싱 메일 폴더(630)를 접속할 때만 나타난다. 반면에, 도 6에서 도시된 실시예에서, 위험한 상태를 나타내는 메타데이터 태그가 첨부된 메시지들(665 및 675)은 인박스 폴더(620) 접속 시에 인박스(680) 내 메시지들(66)의 목록 내에서 나타난다. 즉, 태그된 메시지들과 정당한 메시지들이 공동 저장 장소 내에서 유지되고 인박스 폴더(620)와 같은 공동 폴더 내에서 보관된다. 그래서, 사용자에게 잠재적 피싱 이메일로 식별된 메타데이터 태그가 첨부된 메시지들(665 및 675)의 표현들을 통지하기 위해서, 사용자가 메시지들(665 및 675)을 열어서 보려고 시도할 때 경고 메시지가 표시된다.

[0073] 도 7로 넘어가면, 잠재적 피싱 이메일의 콘텐츠 공개 대신에 렌더링되는 경고 메시지(700)를 나타내기 위한 예시적 사용자 인터페이스의 도해적 스크린 디스플레이가 도시된다. 앞에서 논의된 바와 같이, 두 번째 해결책에

따를 때, 보기 선택이 된 태그된 메시지의 콘텐츠는 비-웹 메일 클라이언트에 의해 사용자에게 디스플레이되는 경고 메시지(700)로 대체된다. 이런 식으로, 경고 메시지는 구체적으로 사용자에게 메시지와 연관된 잠재적 위험을 경고하는 기능을 수행한다. 실시예들 내 경고 메시지(700)는, 선택된 메시지가 위험한 상태와 연관되어있다는 것을 사용자에게 즉시 알리기 위해서 명백한 경고 포스팅(710)을 포함할 수 있다. 더 나아가, 경고 메시지(700)는 본래 콘텐츠를 경고 메시지(700)로 대체하는 것에 대한 설명(720) 및/또는 본래 콘텐츠를 보기 위해서 사용자가 취해야하는 단계들을 명확하게 설명하는 지침들을 포함할 수 있다. 한 예시에서, 지침들은 사용자가 태그된 메시지의 본래 콘텐츠를 보기 위해서 웹 브라우저에 로그인해야한다는 것을 나타낼 수 있다. 이 경우에, 경고 메시지(700)의 본문 내에서는 URL 링크가 제공되지 않는다. 유리하게, URL 링크의 생략을 통해서, 가짜 경고 메시지 내의 URL 링크를 피싱 벡터로 사용하는 부정한 액터(actor)에 대한 어떠한 기회도 방지될 수 있다.

[0074] 다른 예시에서, 도 7에서 도시된 바와 같이, URL 링크(740)는 경고 메시지(700) 안에서 나타난다. URL 링크(740)의 선택은 사용자로 하여금 메시지가 올바르게 잠재적 피싱 이메일로 식별되었는지 여부를 확인할 수 있도록 선택된 메시지의 본래 콘텐츠를 볼 수 있게 한다. 일반적으로, 웹브라우저는 잠재적 피싱 콘텐츠를 여는데 있어서 웹브라우저를 안전한 장소로 만들어주는 안티피싱 제어부들을 포함한다.

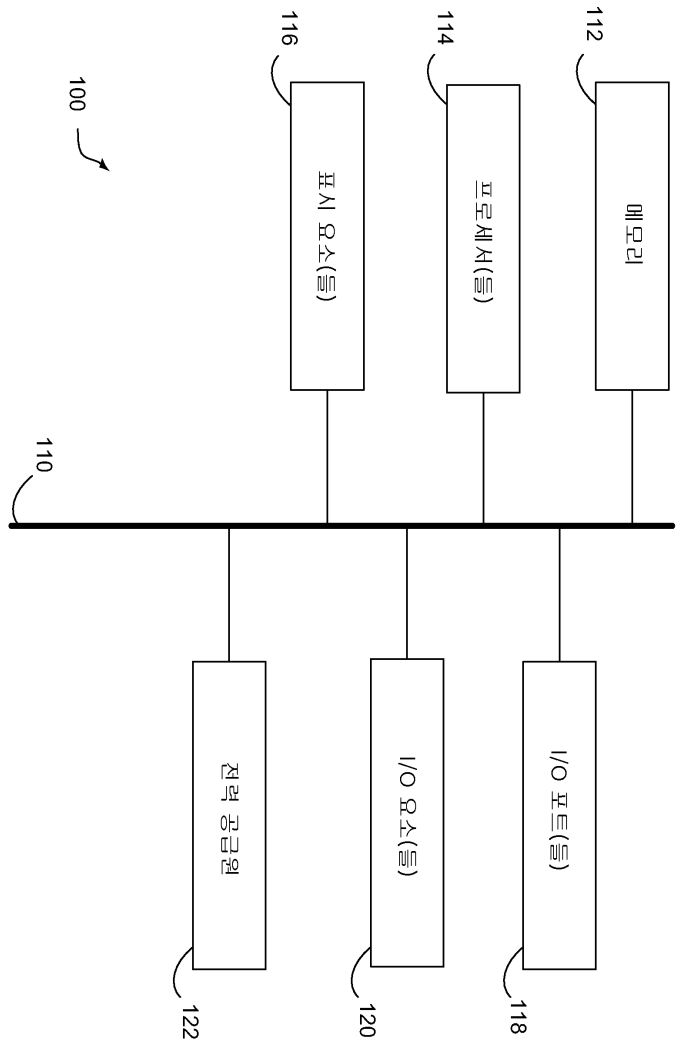
[0075] 또 다른 예시에서, 경고 메시지는 구체적으로 조정된다. 한 실시예에서, 경고 메시지(700)는 태그된 메시지를 읽으려고 시도하는 사용자와 관련된 정보를 기초로 구체적으로 조정되고, 여기서 정보는 서비스 제공자에 의해 접속 가능한 소스들로부터 얻어진다. 예시로써, 경고 메시지(700)의 언어는 사용자와 연관된 지역/시장의 표시를 기초해서 사용자에게 조정되며, 여기서 사용자의 지역/시장의 표시는 사용자의 온라인 프로파일로부터 얻어진다. 두 번째 실시예에서, 경고 메시지(700)는 태그된 메시지와 관련된 정보를 기초로 구체적으로 조정되고, 여기서 정보는 태그된 메시지의 본래 콘텐츠 또는 속성들로부터 얻어진다. 예시로써, 태그된 메시지로부터의 콘텐츠(730) 구절은 경고 메시지(700) 안에서 표시된다.

[0076] 본 발명은 특정 실시예에 관련되어 서술되었고, 이는 제한적이 아닌 도해적 의도이다. 본 발명의 범위를 벗어나지 않고 존재하는 대안적 실시예들이 본 기술의 당업자들에게는 명확하게 인지될 것이다.

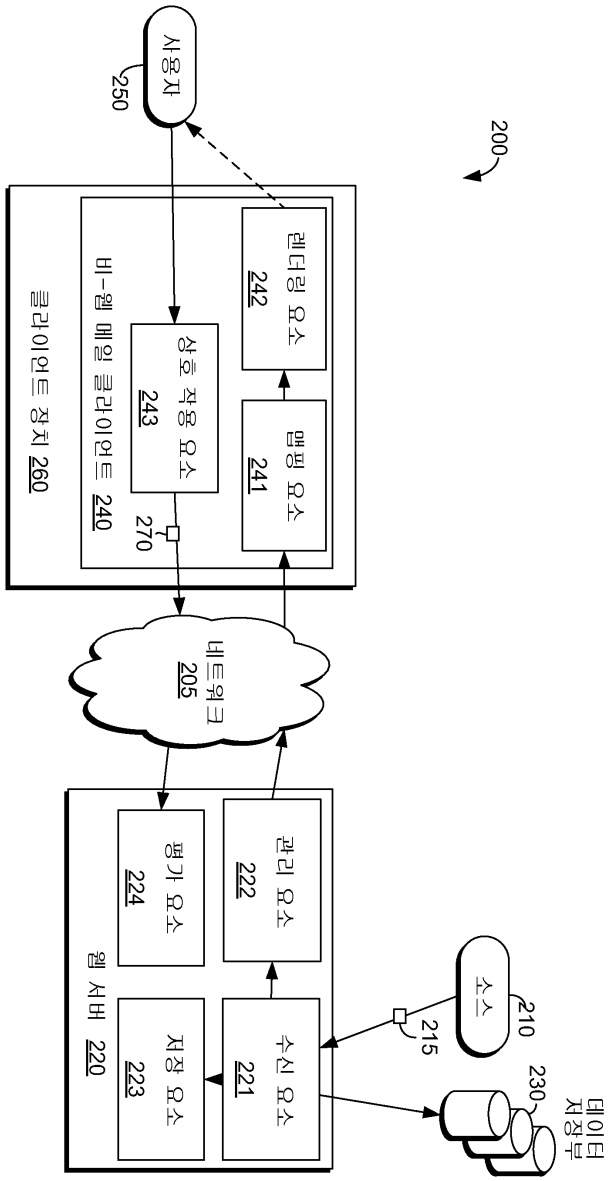
[0077] 앞에서 서술한 바와 같이, 본 발명이 시스템 및 방법들에게 자명하고 고유한 다른 장점들과 함께, 위에서 서술된 모든 목적들 및 객체들을 취득하는데 적합하다는 것을 이해할 수 있을 것이다. 특정 기능들과 부-결합들(sub-combination)은 활용성이 있고 다른 기능 및 부-결합들과의 관련 없이도 적용될 수 있다. 이는 청구항들의 범위에 의해 그리고 그 안에서 고려된다.

도면

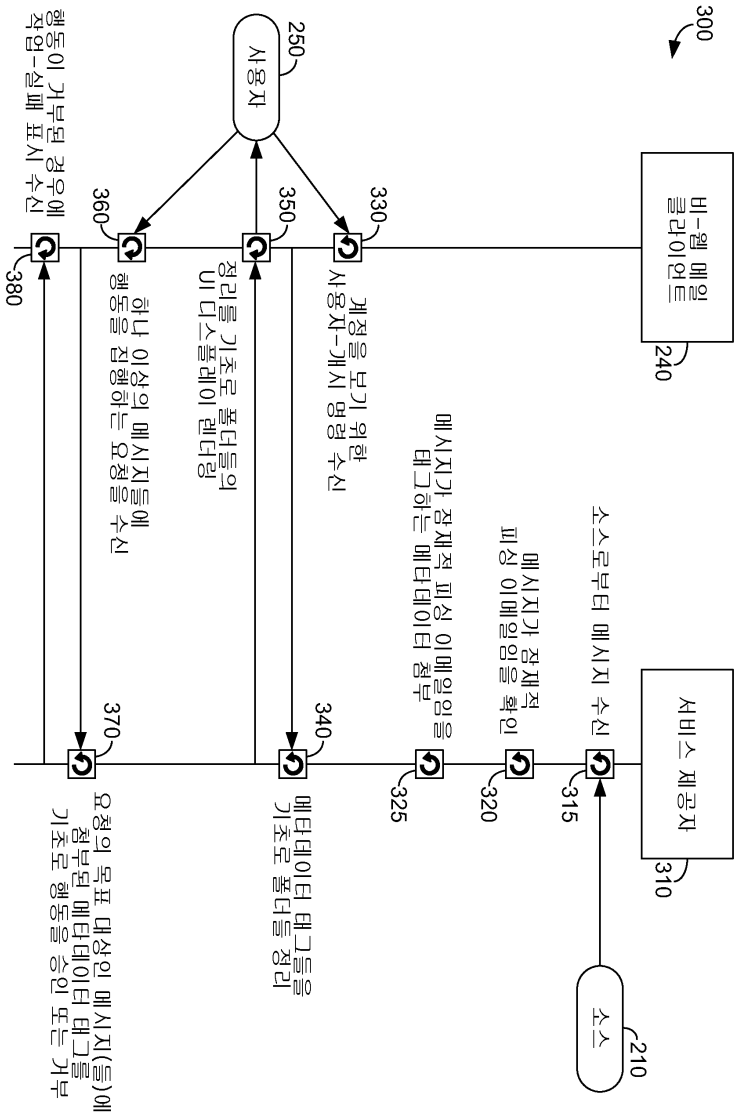
도면1


100
110
112
메모리
114
프로세서(들)
116
표시 요소(들)
118
I/O 포트(들)
120
I/O 요소(들)
122
전력 공급원

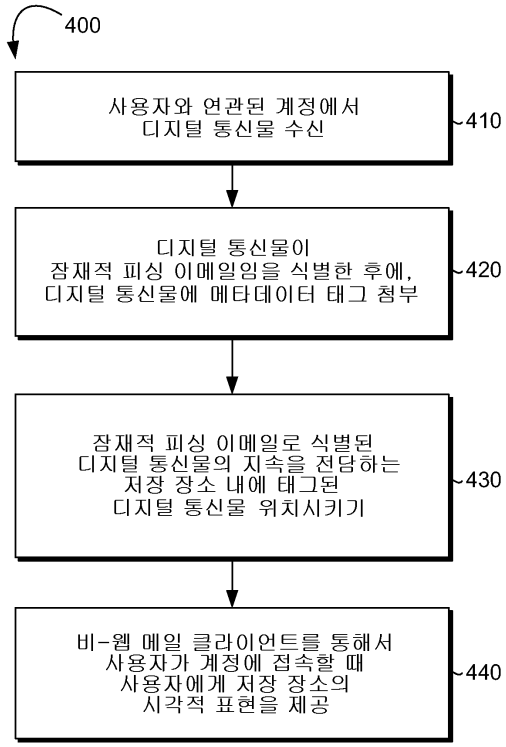
도면2


200
사용자
250
클라이언트 장치 260
비-웹 메일 클라이언트 240
렌더링 요소
242
맵핑 요소
241
상호 작용 요소
243
270
네트워크
205
웹 서버 220
관리 요소
222
평가 요소
224
수신 요소
221
저장 요소
223
소스
210
215
230
데이터 저장부

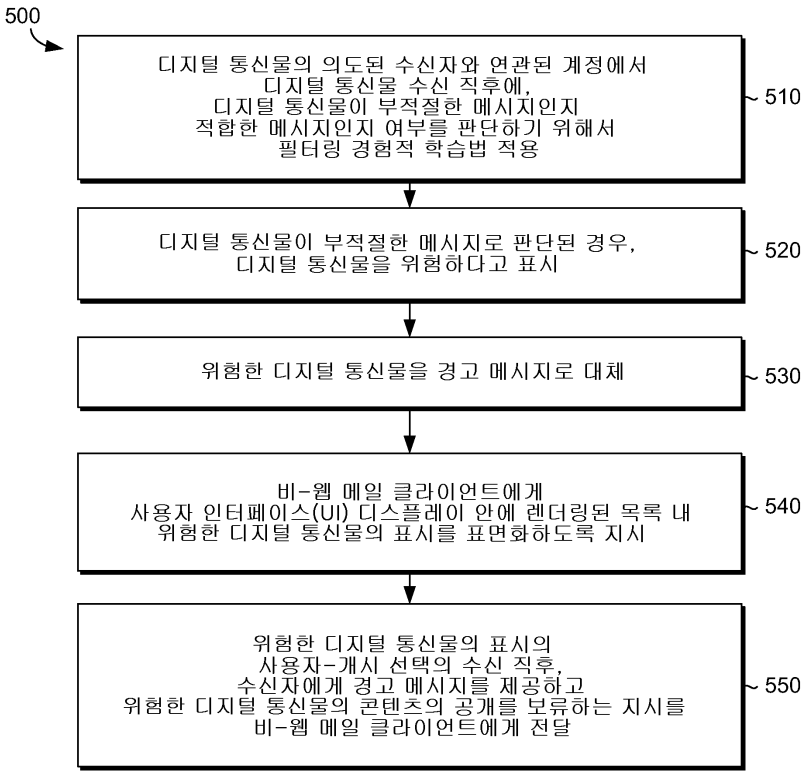
도면3


300
비-웹 메일 클라이언트
240
서비스 제공자
310
소스
210
315
320
325
330
340
350
360
370
380
사용자
250
소스로부터 메시지 수신
메시지가 잠재적 피싱 이메일임을 확인
메시지가 잠재적 피싱 이메일임을 태그하는 메타데이터 첨부
계정을 보기 위한 사용자-개시 명령 수신
정리를 기초로 폴더들의 UI 디스플레이 렌더링
하나 이상의 메시지들에 행동을 집행하는 요청을 수신
메타데이터 태그들을 기초로 폴더들 정리
요청의 목표 대상인 메시지(들)에 첨부된 메타데이터 태그를 기초로 행동을 승인 또는 거부
행동이 거부된 경우에 작업-실패 표시 수신

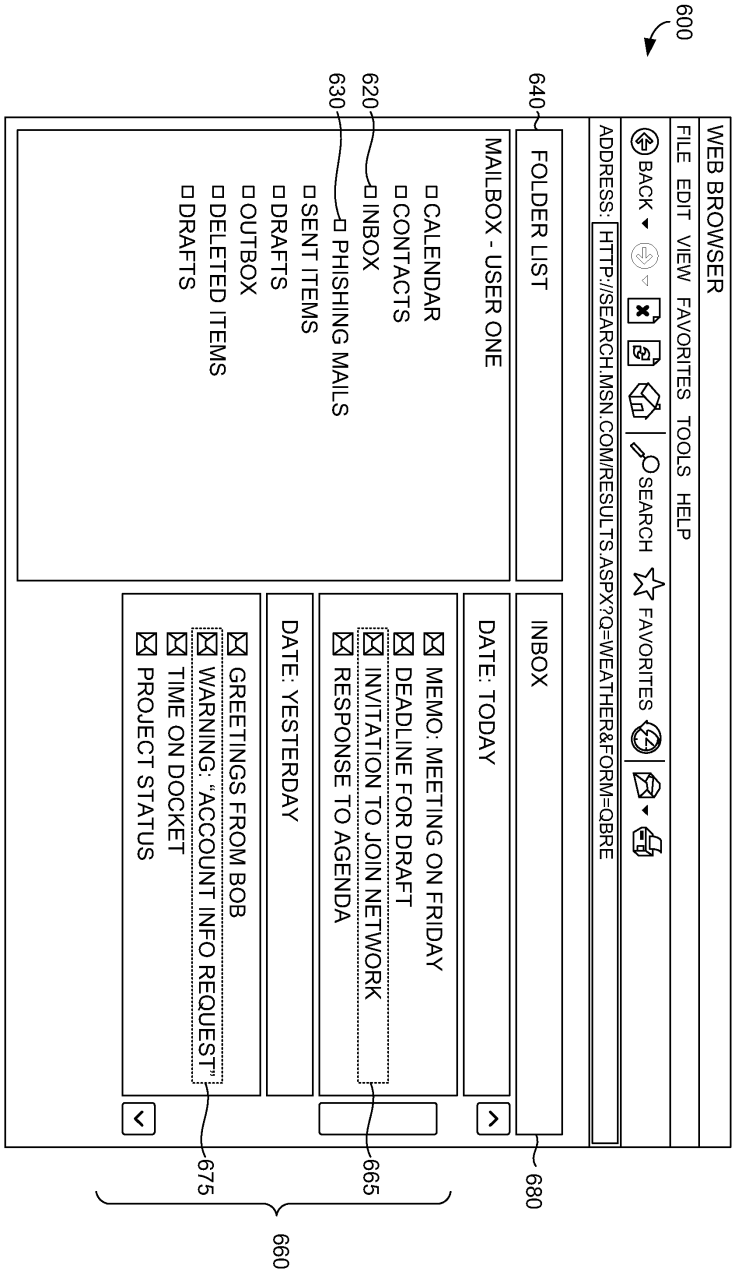
도면4


400
사용자와 연관된 계정에서
디지털 통신물 수신
410
디지털 통신물이
잠재적 피싱 이메일임을 식별한 후에,
디지털 통신물에 메타데이터 태그 첨부
420
잠재적 피싱 이메일로 식별된
디지털 통신물의 지속을 전담하는
저장 장소 내에 태그된
디지털 통신물 위치시키기
430
비-웹 메일 클라이언트를 통해서
사용자가 계정에 접속할 때
사용자에게 저장 장소의
시각적 표현을 제공
440

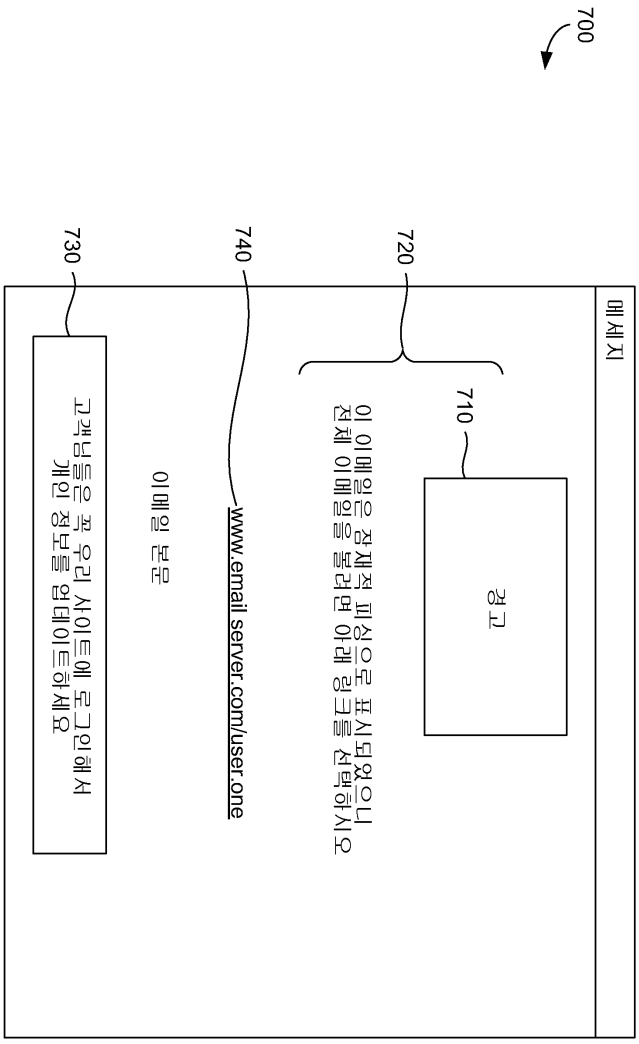
도면5


500
디지털 통신물의 의도된 수신자와 연관된 계정에서
디지털 통신물 수신 직후에,
디지털 통신물이 부적절한 메시지인지
적합한 메시지인지 여부를 판단하기 위해서
필터링 경험적 학습법 적용
510
디지털 통신물이 부적절한 메시지로 판단된 경우,
디지털 통신물을 위험하다고 표시
520
위험한 디지털 통신물을 경고 메시지로 대체
530
비-웹 메일 클라이언트에게
사용자 인터페이스(UI) 디스플레이 안에 렌더링된 목록 내
위험한 디지털 통신물의 표시를 표면화하도록 지시
540
위험한 디지털 통신물의 표시의
사용자-개시 선택의 수신 직후,
수신자에게 경고 메시지를 제공하고
위험한 디지털 통신물의 콘텐츠의 공개를 보류하는 지시를
비-웹 메일 클라이언트에게 전달
550

도면6


600
WEB BROWSER
FILE EDIT VIEW FAVORITES TOOLS HELP
BACK
SEARCH
FAVORITES
ADDRESS: HTTP://SEARCH.MSN.COM/RESULTS.ASPX?Q=WEATHER&FORM=QBRE
640
FOLDER LIST
MAILBOX - USER ONE
CALENDAR
CONTACTS
620
INBOX
630
PHISHING MAILS
SENT ITEMS
DRAFTS
OUTBOX
DELETED ITEMS
DRAFTS
INBOX
680
DATE: TODAY
MEMO: MEETING ON FRIDAY
DEADLINE FOR DRAFT
INVITATION TO JOIN NETWORK
RESPONSE TO AGENDA
665
DATE: YESTERDAY
GREETINGS FROM BOB
WARNING: "ACCOUNT INFO REQUEST"
675
TIME ON DOCKET
PROJECT STATUS
660

도면7


700
메세지
710
경고
720
이 이메일은 잠재적 피싱으로 표시되었으니
전체 이메일을 살펴보면 아래 링크를 선택하시오
740
www.email.server.com/user.one
이메일 본문
730
고객님들은 꼭 우리 사이트에 로그인해서
개인 정보를 업데이트하세요