# Phishing Attacks in a Mobile Environment

Saeed Abu-Nimeh and Suku Nair

SMU HACNet Lab
Southern Methodist University
Dallas, TX
{sabunime,nair}@engr.smu.edu

**Abstract**

There is no agreed upon definition for Phishing. Although, the medium of attack may vary, the goal is to steal confidential information from an individual. Classical Phishing attacks via mass mailing have a low return of investment rate. Generally, one mass mailing of 100,000 emails may collect between 10 to 100 victims. On the contrary, Phishing scams targeted to a specific group of people in a certain time, dubbed by ”Spear Phishing”, have higher success rate. Mobile environment provides an optimum atmosphere for such scams to succeed. The present study shows new media of Phishing attacks other than traditional emails scams. The study presents how Wi-Fi, Bluetooth, mobile applications, and RFID facilitate and increase the potential of success in Spear Phishing. Further, we discuss Phishing examples and show that available defense solutions against Phishing attacks are inadequate in a mobile environment. Therefore, alternatives have to be deemed to fit mobile architectures and applications.

## Keywords

Phishing, Spear Phishing, Pharming, Evil Twin, Web Spoofing, Bluetooth, Wi-Fi, RFID, Windows CE, Symbian OS.

## 1 Introduction

Phishing was first used in 1996 by hackers to steal America Online (AOL) accounts by scamming passwords from AOL users [51]. Web spoofing was first mentioned by Felten et al. [26]. They showed that an attacker can create shadow copy of the World Wide Web and monitor user activities including passwords and account numbers. Should the attack succeed, the attacker can send false or misleading data in the victims name. Today, the Anti-Phishing Working Group (APWG) [1] defines Phishing as a form of online identity theft that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. According to the Department of Homeland Security (DHS) report [24] Phishing is online identity theft in which confidential information is obtained from an individual. In [37], the author defines Phishing as the act of sending a forged e-mail to a recipient, falsely mimicking a legitimate establishment in an attempt to scam the recipient into divulging private information such as credit card numbers or bank account passwords.

In their Phishing activity trends report, the APWG received 16882 unique Phishing reports in November 2005 showing an increase of 88% in the total number of unique Phishing reports submitted in November 2004. Figure 1 shows the number of unique Phishing reports submitted to the APWG between November

2004 and November 2005 [30]. According to the same report, 32.96% of Phishing websites are hosted in the Uniter States. In 2003 direct Phishing-related loss to US banks and credit card issuers was estimated by $1.2 billion [24]. According to the annual AOL/National Cyber Security Alliance (NCSA) Online Safety Study [52], Phishing attacks now affect almost one in four Americans each month. The survey showed that more than two-thirds of consumers who received Phishing emails thought they were from legitimate companies. In addition, the study reported that one in five users had a friend or family member fallen a victim to an online identity theft scam. All of these figures show that Phishing is on the rise and solutions need to be proposed and implemented.

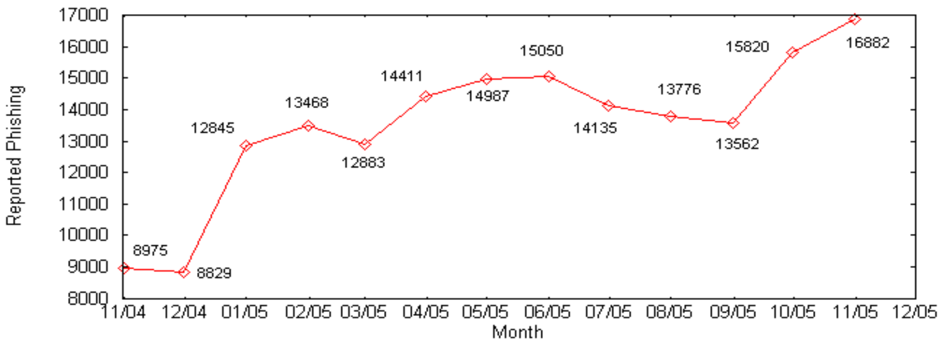


Figure 1: Unique Phishing reports submitted to the APWG.

Similar to the rise in Phishing attacks, there has been a staggering rise in the usage of mobile devices, Wi-Fi, Bluetooth, and Radio Frequency IDentifier (RFID) tags. Users are using blackberries, Personal Digital Assistants (PDAs), even cell phones to access their bank accounts and store sensitive personal data. According to JiWire [38] there are more than 50,000 Wi-Fi hotspots in the world today. This number is expected to increase to 200,000 by 2008. The total revenue of WLAN equipment is estimated to be $4.3 billion in 2009 as revealed by the Dell'Oro Group [31]. Companies are using RFID tags in building smart home appliances, such as: washing machines and refrigerators [39]. Washing machines would be able to select wash cycles automatically to avoid damage to delicate fabrics and refrigerator would be able to give a warning when the milk has expired or could transmit a shopping list automatically to a home delivery service. Grocery stores are also planning to use RFID tags to store customer's information as it will be easier for them to track their customers and send them promotions for goods and services they prefer [29]. In addition, hospitals are planning to use RFID tags in medication compliances and health care systems [28]. Bluetooth-enabled devices such as: cell phones, PDAs, laptops, and blackberries have been used abundantly as well. According to the Bluetooth annual report [61], producers of devices containing Bluetooth technology shipped four million units per week in September of 2004. In fall 2004 a survey studied the consumer recognition and awareness of Bluetooth wireless technology in the UK, Japan, and the US. The study showed that 77% in the UK, 61% in Japan, and 41% in the US recognize and are aware of Bluetooth technology. All of these mobile applications and architectures are making the life of users easy and fast, however, a key question is the feasibility, security, and privacy of such technologies. Many have raised concerns over the privacy implications of these technologies.

Our study proves that Phishing attacks are not only achieved by mass mailing victims or DNS (Domain Name Service) poisoning and hijacking. Attackers can steal personal identity data from cell phones, blackberries, and PDAs using other techniques. Our contribution shows that Phishing attacks are apparent and likely to occur in a mobile environment. Mobility has a vital role and gives an advantage to the attack to succeed presumably the attack is targeted to a specific group in a specific time, which is known by Spear Phishing. The study shows that in some cases it takes less effort to convince the victim of the legitimacy of the attack. However, in other cases exploiting vulnerabilities that already exist in Wi-Fi, Bluetooth, Mobile operating systems, or RFID would be an advantage to the attacker. The rest of this paper is organized as follows: Section 2 discusses related and previous work in Phishing detection. Section 3 presents Phishing attack scenarios in a different mobile applications and architectures. We propose recommended defense mechanisms in section 4. In section 5 we draw conclusions and motivate for future work.

## 2 Related Work

There has been a lot of work done in Phishing detection. We discuss solutions proposed by vendors and researchers in Phishing detection and prevention. We discuss research proposals in details, however, we only list vendor solutions as it is hard to get a detailed illustration of these solutions and tools for vendor privacy issues. Phishing fraud solutions and defense mechanisms can be divided into three main categories [37] as illustrated in Table 1.

Table 1: Phishing and fraud solutions.

| Detective solutions | Preventive solutions | Corrective solutions |
|---|---|---|
| Monitors account life cycle<br>Brand monitoring<br>Disables web duplication<br>Performs content filtering<br>Anti-Malware<br>Anti-Spam | Authentication<br>Patch and change management<br>Web application security | Site takedown<br>Forensics and investigation |

Account monitors are used to track identity behavior of an account from opening through the entire account lifecycle. Examples of such solutions are: AutoTrackXP by ChoicePoint [14], , National Fraud Database by Experian [25], Identity Risk management by ID Analytics [6], LexisNexis [41], Qsent [55], Fraud Protection by Verisign [67], and Bharosa Tracker by Bharosa [10]. Similarly, Brand monitors are used to notify customers of URL spoofing and misspelled domain registrations. For instance: Threat and Fraud Management by Cyveillance [20], and VigilActive by NameProtect [46].

Fraud Detection System by Corillian [18] is an example of solutions that detect fraudulent websites using web duplication detectors. Strike Phish by Brandimensions [12], Powershark by Internet Identity [34], FraudAction by Cyota [19], Fraud Protection by MarkMonitor [42], and SLAM by Secure Science [58] are examples of brand monitoring, site takedown, forensics, and investigation solutions. Cyota also has eVision for account lifecycle monitoring and eSphinx for duplicate site detection.

Content filters (proxy servers) and toolbar add-ins detect fraudulent URLs and alert users or identify trusted sites. Toolbar add-ins include: Cloudmark Anti Fraud Toolbar [16], Scam Alarm by CollectiveTrust [17], ScamBlocker by Earthlink [23], TrustWatch Toolbar [66], Anti-Phishing Toolbar by Netcraft [47], Web Caller-ID by Symantec [13], TippingPoint IDS [63], SpoofStick [62], and IE Phishing filter by Microsoft [43]. Proxy servers include: 0proxy by 0spam.net [2], Anonymous Surfing by Anonymizer [7], FortiGuard Web Content Filtering by Fortinet [27], and WebTunnel by Primedius [54].

In addition, researchers have contributed to Phishing detection. Some solutions have been proposed in designing and implementing security toolbars or web browser add-ons. Chou et al. [15] proposed SpoofGuard a client-side toolbar to detect web spoofing and Phishing. The tool gives a score to each message at the retrieval step. The score is given based on common characteristics of the previous detected Phishing attacks. Examples of characteristics used: misleading patterns in URLs and password input fields in page with no secure connection. Based on the score, the tool provides a light (red, yellow, and green) in a toolbar indicating if the page is spoofed or not. Should the tool not determine if the page is spoofed or not, it asks for user input. Herzberg and Gbara [33] proposed TrustBar a browser add-on to Mozilla Firefox browser. The toolbar identifies the site and the certificate authority (CA), using logos or names rather than testing the URL itself. For unprotected pages, If a spoofed page is detected TrustBar displays highly visible warnings on the browser window.

Wu et al. [70] evaluated the effectiveness of security toolbars in preventing Phishing attacks. They performed experiments on three security toolbars, the browsers address bar, and the status bar. A total of 30 subjects were included in experiments. They showed that all tested security toolbars were ineffective in preventing Phishing attacks. Users were spoofed 34% of the time. 20 out of 30 users got spoofed by at least one Phishing attack. 85% of the spoofed users thought that websites look legitimate or exactly the same as they visited before. 40% of the spoofed users were tricked because of poorly designed websites, especially when using improper redirections. In consequence the study concludes that there are two main reasons behind the users failing into these attacks: First, users discarded the toolbar display as the content of web pages looks legitimate or professional. Second, many companies do not follow good practice in designing their websites and the toolbar cannot help users to distinguish poorly designed websites from malicious phishing attacks.

Dhamija and Tygar [21] proposed Dynamic Security Skins as an extension to Mozilla Firefox browser. The browser extension provides a trusted window in the browser dedicated to username and password using a photographic image to create a trusted path between the user and the window. A unique abstract image for each user and each transaction is generated by the remote server which users connect to. This image is placed as a skin to the browser window or the user interface. The proposal has a very low overhead on the user in terms of effort, memory and time.

Wenyin et al. [68] proposed a Phishing detection technique based on visual similarity. Webpages are decomposed into salient blocks according to visual cues. Three aspects are measured to find similarities between the pages: First, block level similarity where the content of a block can be categorized as either text or image. Second, layout similarity where the layout similarity is defined as the ratio of the weighted number of matched blocks to the total number of blocks in the true webpage. Third, overall style similarity which can be represented by format definitions, such as: fonts, background color, text alignment, and line spacing. A threshold is fixed to determine that the webpage is Phishing if the similarities exceed it. Obviously, depending on the threshold level, false alarms could exist.

ViWiD [59] is a server-side watermarking based approach, which checks the integrity of website logo using visible watermarking. The watermark message is unique for every user, which consists of the date and local time of the day for the users time zone, and the users mnemonic. In addition, the watermark message carries a shared secret between the company and the user. User are required to expect a valid message to be displayed on the logo images when they perform sensitive transactions.

Jakobsson [35] provided a graphical model of Phishing attacks. A Phishing graph is a directed graph in which nodes correspond to knowledge or access rights and edges correspond to means of obtaining information or access rights either legally or illegally. Edges are weighted with probabilities, costs, or other measures of the hardness of traversing the graph. Using this model economic analysis can be performed on the viability of attacks to improve weak links that will eventually help in improving overall system security. In addition, Jakobsson proposed context aware Phishing attack. This attack is held using messages that from their context are expected and accepted by victims. The attack takes advantage of linking victim identities and email addresses or what is called identity linking. Jakobsson and Young proposed Distributed Phishing Attacks (DPA) [36] to shut down sites run by Phishers. The attack consists of three programs: the transmitter application, the transponder cryptotrojan, and the receiver application. The attack works by a per-victim personalization of the location of sites collecting credentials and a covert transmission of credentials to a hidden coordination center run by the Phisher. A Secure public key steganography assures that the stego channel is not detected, and the broadcast channel ensures that the Phisher is not identified when reading the broadcast.

Adida et al. [3] proposed Lightweight Trust Architecture (LTA) a solution to the email-based Phishing. The solution consists of two steps: First, the design of a lightweight public-key infrastructure to distribute identity-based public keys using existing hardware and software architectures. Second, the use of repudiable identity-based signatures that convince an email recipient of the senders authenticity, without allowing that recipient to prove this authenticity to any third party. In addition, same authors [4] proposed Separable Identity-Based Ring (SIBR) signatures a solution to email spoofing problem. In their proposal full Public-Key Infrastructure (PKI) is not needed, since they use identity-based public keys. Separability allows ring constructions across different identity-based master key domains, thus email senders and recipients can belong to different domains. Using this scheme, email senders can create an ad-hoc group signature using a signatory group. Senders can derive recipients' public key directly from the email address and some basic DNS information.

Sanitizing Proxy System (SPS) is proposed in [44]. The system can be implemented in as proxy system in a personal firewall or a browser plug-in. The system removes parts of the HTML content that traps novice users into entering their personal identity data. The system consists of two-level filtering: Strict URL Filtering (SUF) and HTTP Response Sanitizing (HRS). SUF checks the source of the HTTP response against a rule-set of prioritized allow/deny rules. In contrary to firewalls, SUF does not block traffic, it only distinguishes safe URLs from other suspicious URLs then it applies HRS to every HTTP responses from suspicious URLs. HRS replaces malicious HTTP headers and HTML tags with warning messages. By doing this, HRS alerts novice users about the malicious parts in a webpage that is attempting to steal their personal information.

# 3 Phishing Attacks in a Mobile Environment

In this section we provide detailed discussion on four Phishing attack scenarios in a mobile environment. We show attack scenarios in Wi-Fi architecture, attacks on Bluetooth applications, attacks on pocket PCs running Windows Mobile (CE), and attacks on RFID tags.

## 3.1 Wi-Fi Phishing attack scenario

Most wireless LANs are based on the IEEE 802.11 standard, better known as Wi-Fi. 802.11b and 802.11g equipment operate in the same 2.4-GHz band. However, 802.11a equipment operate in the 5.0-GHz band. A Wi-Fi home router using 802.11b or 802.11g might have a range of 45 m indoors and 90 m outdoors [22]. Concerns have been raised regarding security issues in Wi-Fi. Man in the middle attacks at layer one of the OSI model are difficult to discover. Specifically in Wi-Fi, it is hard to find out that the attack occurred. Many users are leaving their wireless Access Points (AP) open (unsecured). If an attacker uses a simple sniffer, such as: Ethereal [48], he would be able to sniff the traffic and get the data as plain text. If the user uses a secure connection such as: WPA, WEP, SSL, or SSH, the traffic would be of no value in this case. However, if the attacker succeeds in inducing the user to a non-SSL-protected server, all of the victims credentials and personal identity data will be exposed. The attacker can direct the user to an unsecured server by using *Evil Twins* [49, 50] or *cousin SSIDs* (Service Set IDentifier). In Wi-Fi it is easy to set up a fake AP as users can not validate the authenticity of access points they are connecting to. Hence, the attacker can setup an AP with SSID that looks like it ought to be a legitimate one. For example he creates an AP near Starbucks with a cousin SSID: Starbucks_WiFi or a generic name like ”Linksys”, ”Wireless”, or ”Hotspot”. The attacker may also jam the connection to the legitimate AP by sending a stronger signal within close proximity to the wireless victim. Once the victim is connected to the Evil Twin, the attacker gets all of his personal information and credentials such as: bank accounts, passwords, and credit card numbers. Pharming is another attack that can occur using a rogue AP. In this case the attacker misdirects users to fraudulent sites or proxy servers, through DNS hijacking or poisoning. After setting up the Evil Twin, the attacker provides the victim with an IP address, a gateway, and a DNS. Thus, he will be able to resolve all URLs and address, using fake DNS replies . As a result, Phishing websites are displayed instead of legitimate ones.

As a proof-of-concept, the Shmoo group released Airsnarf [57], a rogue wireless access point setup utility. Airsnarf demonstrates how a rogue AP can steal personal identity data from public wireless hotspots. Airsnarf creates a competing hotspot with a configured local network, gateway, and SSID. Like any other hotspot Wireless clients that associate to Airsnarf access point receive an IP, DNS, and gateway. Despite of users’ DNS settings, all DNS queries resolve to a provided IP. Thus, all URL queries bring up the Airsnarf ”splash page”, requesting a username and password. In consequence, victims’ collected data is emailed to `root@localhost`.

In the following attack scenario ”Alice” is having her morning coffee at Starbucks. While she is setting there, she uses ”Starbucks” hotspot to surf the web. However, ”Bob” set up a rogue AP ”Starbucks_WiFi” with a stronger signal range. DNS entries in the rogue AP are poisoned to direct to Phishing websites instead of legitimate financial institutions and other common used URLs. ”Alice” connects to ”Bank X” website to pay some bills. A Phishing website opens looking exactly like the legitimate one and the address bar is showing the correct Bank X URL as well. ”Alice” finishes her coffee and leaves to work. In the mean while, ”Bob” phished her and is waiting for his next customer. Figure 2 illustrates the Wi-Fi Phishing attack.

Automatic Wireless Network Selection [71] demonstrates vulnerabilities in how Windows XP and MacOS X workstations automatically identify and join wireless networks. KARMA [69] is a proof-of-concept toolkit that demonstrates the risk of such vulnerabilities through a patch to the Linux MadWifi driver and client-side exploit toolkit. The driver responds to every probe request as it operates in HostAP mode. When a client in range sends a probe request for a network, such as: ”Tmobile” or ”Linksys”, the driver acts as a virtual AP and responds as if it were that network. Similar to the previous attack, however without setting up an Evil Twin, all un-associated wireless clients within range will join the rogue virtual network. Thus, the attacker can redirect users’ traffic to Phishing websites in order to steal their personal information. The authors of the toolkit demonstrated the attack in a security conference [1]. They were able to hijack 100 laptops out of almost 400 attendees.

[1] First BlueHat security conference

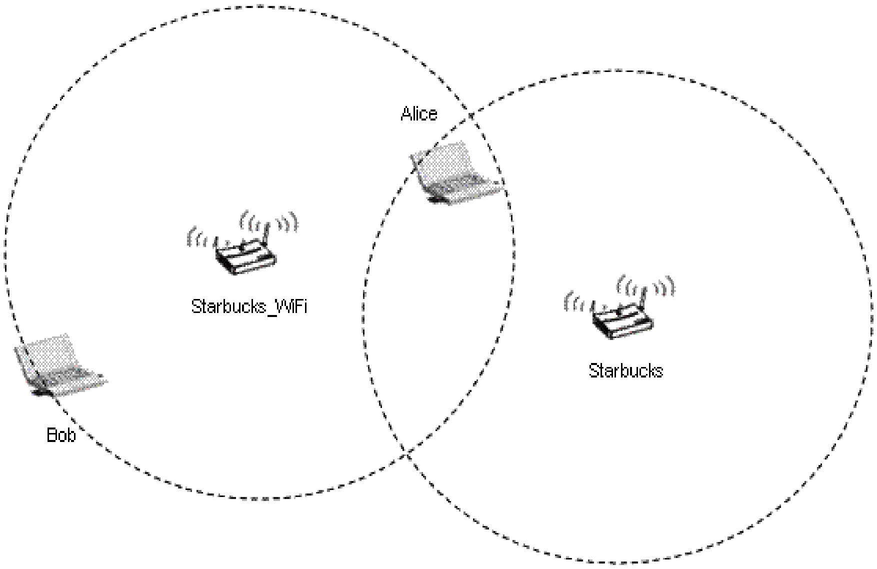


Figure 2: Wi-Fi Phishing attack flow.

### 3.2 Bluetooth Phishing attack scenario

Bluetooth [60] is a short range wireless data and two-way voice transfer technology providing data rates up to 3 Mb/s. It operates using frequency hoping at 2.4 GHz frequency in the free ISM band (Industrial Scientific Medicine). Recently, Bluetooth-enabled devices have had concerns regarding their security. Bluetooth-enabled phones have serious security flaws that allow attackers to connect to the device without users' permission. The SNARF [40] attack enables access to restricted areas of the device. The attacker can get access to the victims's phone book database either stored on the phone or the SIM card. In addition, the attacker can get access to the calendar, to-do list, and lists of missed and received calls. It is also possible to retrieve and send SMS messages from the victim's device or to initiate phone calls to any existing contact [32]. Accordingly, the attacker can send all of these information back to him or to other Bluetooth-enabled devices in range.

Blooover [64] is a proof-of-concept tool which runs on J2ME-enabled cell phones that exploits Bluebug. Bluebug is the name of a bluetooth security loophole on some bluetooth-enabled cell phones. It allows the attacker to not only initiate phone calls from the victim's device, but also eavesdrop on the victim calls when the victim passes by. Moreover, the attacker can read/write phone book entries, download call lists, set call forwarding, connect to the internet, and send/read SMS messages from the attacked phone. In consequence, The attacker can figure out the victim's phone number by sending himself an SMS message from the victims's device. The attacker should be in 10-15 meter range of the victim due to the limited transmit power of class 2 bluetooth radios [65].

In addition, there are applications that exploit and get access to Bluetooth-enabled devices. For instance, `Pbstealer.A` is a trojan application that runs under Symbian Series 60 platform. It pretends to be utility software that compacts the phone contacts database. However, it reads the contact information database, and sends the contents as text file to first bluetooth device it finds. If the user installs the `sis` package that contains `Pbstealer.A`, the device will be infected [53].

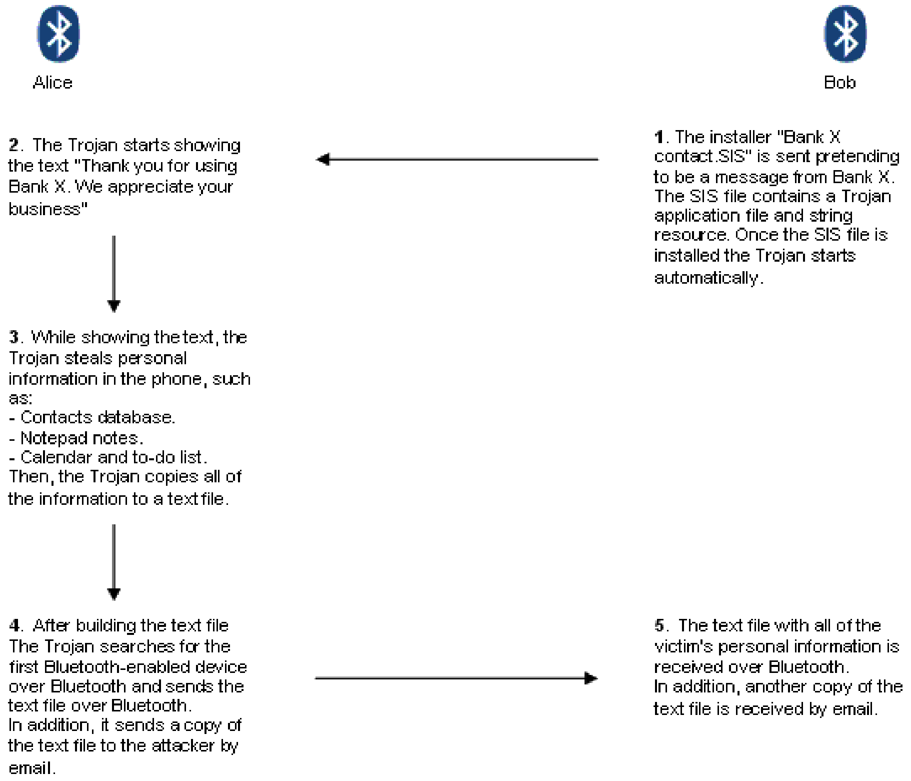

Alice
Bob
1. The installer "Bank X contact.SIS" is sent pretending to be a message from Bank X. The SIS file contains a Trojan application file and string resource. Once the SIS file is installed the Trojan starts automatically.
2. The Trojan starts showing the text "Thank you for using Bank X. We appreciate your business"
3. While showing the text, the Trojan steals personal information in the phone, such as:
- Contacts database.
- Notepad notes.
- Calendar and to-do list.
Then, the Trojan copies all of the information to a text file.
4. After building the text file The Trojan searches for the first Bluetooth-enabled device over Bluetooth and sends the text file over Bluetooth.
In addition, it sends a copy of the text file to the attacker by email.
5. The text file with all of the victim's personal information is received over Bluetooth.
In addition, another copy of the text file is received by email.

Figure 3: Bluetooth Phishing attack flow.

A Bluetooth Phishing scenario can be as follows: ”Alice” has a Bluetooth-enabled cell phone and she leaves her phone to accept bluetooth transfer by default. She is a regular customer of ”Bank X”. Out of ”Bank X”, ”Bob” is waiting in his car, Snarfing for customers using bluetooth-enabled devices, while they are leaving the bank. ”Alice” leaves ”Bank X”, ”Bob” detects ”Alice’s” device and sends a Phishing attack to her cell phone. ”Alice” receives the file ”Bank X contact.sis” while she is walking out. ”Alice” opens the *sis* file and the trojan starts automatically. Figure 3 illustrates the trojan flow from running the application till ”Bob” receives ”Alice’s” personal information.

In Program 1, we show a proof-of-concept code [2] snippet that demonstrates a Phishing attack on a Bluetooth phone running Symbian Series 60 platform. The trojan extracts the contacts database, the notepad files, and the calendar and to-do list. The trojan emails and sends the information via Bluetooth to the attacker in a text file [9].

### 3.3 Windows CE Phishing attack scenario

A hand-held device can be described as a pocket sized device with computing capabilities. This includes: PDAs, PocketPCs, smartphones, blackberries, etc. Hand-held devices are used as personal organizers of contact lists, calendar of events, voice recorder, notes, and more [45]. Most of these devices have basic limitations such as: limited screen size, low battery life, small storage space, operating system installed with

[2] Code is provided by MARA

**Program 1** Bluetooth Phishing proof-of-concept code.

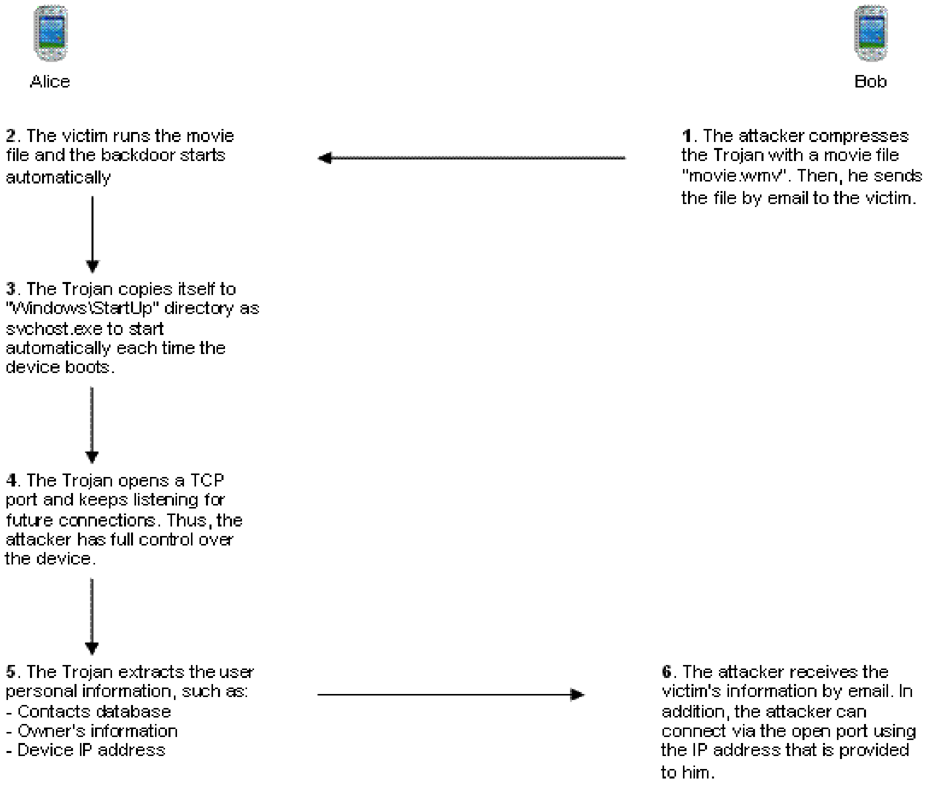
```
   //Open contacts database and copy to a list
    CContactDatabase* database;
    database = CContactDatabase::OpenL();
    CleanupStack::PushL(database);
    const CContactIdArray* contacts = database->SortedItemsL();

    //write notepad.dat into a text file
    writer.WriteL(text);
    RFile notepadfile;
    notepadfile.Open(iCoeEnv->FsSession(), NotepadFilestr, EFileRead);
    RFileReadStream reader1(notepadfile);
    reader1.ReadL(writer);
    reader1.Close();
    notepadfile.Close();

    //write calendar and to-do list into a text file
    writer.WriteL(text);
    RFile calendarfile;
    calendarfile.Open(iCoeEnv->FsSession(), CalendarFilestr, EFileRead);
    RFileReadStream reader2(calendarfile);
    reader2.ReadL(writer);
    reader2.Close();
    calendarfile.Close();
```

limited resources, and reduced processing capabilities [56]. More important, PocketPCs running Windows CE have equal access privileges to all users. In addition, these devices lack strong anti-virus protection [45]. Moreover, searching the registry of these devices to extract personal information is not challenging.

Brador is the first known backdoor for the Pocket PC hand-held devices. The trojan copies itself to startup folder `Windows\StartUp` as `svchost.exe` to start automatically each time the device reboots. In addition, Brador reads the local IP address of the device and mails it to the attacker. Moreover, the backdoor opens a TCP port 2989, hence the attacker can connect and have full control over the device.
In this attack scenario, ”Alice” uses a Pocket PC with Windows CE OS with a weak anti-virus protection. She uses her phone to send and receive emails. ”Bob” plans to steal ”Alice's” contact database and some personal information from her Pocket PC. He compresses a trojan in a video file and emails the video file to ”Alice”. Figure 4 demonstrates the attack scenario on ”Alice's” Pocket PC.

In Program 2 we modify Brador's code [8] to steal the contacts database from the pocket pc. Accordingly, our trojan sends the contacts database along with the device IP address similar to Brador [3].

[3] Code provided by Jose Andre Morales from MARA



1. The attacker compresses the Trojan with a movie file "movie.wmv". Then, he sends the file by email to the victim.

2. The victim runs the movie file and the backdoor starts automatically

3. The Trojan copies itself to "Windows\StartUp" directory as svchost.exe to start automatically each time the device boots.

4. The Trojan opens a TCP port and keeps listening for future connections. Thus, the attacker has full control over the device.

5. The Trojan extracts the user personal information, such as:
- Contacts database
- Owner's information
- Device IP address

6. The attacker receives the victim's information by email. In addition, the attacker can connect via the open port using the IP address that is provided to him.

Figure 4: WinCE Phishing attack flow.

### 3.4 RFID Phishing attack scenario

Radio-Frequency IDentification (RFID) is a general term for small, wireless devices that emit unique identifiers upon interrogation by RFID readers [11]. RFID tags are small microchips designed for wireless data transmission. Generally, they don't have on-board power source (passive RFID tags), thus they derive their transmission power from the signal of an interrogating reader. Passive tags have read ranges from half a meter up to tens of meters depending on their frequency range [39]. Electronic Product Code (EPC) tags –a form of RFID tags– are used in commercial supply chains due to their cheap price (five cents/unit in large quantities). Interestingly, the basic EPC tag does not have any digital authentication as it lacks sufficient circuitry to implement even symmetrickey cryptographic primitives [11].

According to [39], RFID tags have two main privacy concerns: clandestine tracking and inventorying. RFID tags can be tracked as they respond to any reader interrogation without alerting their owners by broadcasting a unique identifier and fixed serial number to nearby readers. In addition, EPC tags are subject to inventorying and Phishing attacks as they carry information about the items to which they are attached. An ultimate Phishing attack occurs in ”loyalty cards” where the tag serial number is combined with personal information. The attacker with an RFID reader can stealthily steal the victim's address, types of medications he uses, and what illnesses he may suffer from. All these information can be stolen due to poor security protection in these RFID tags. An attack scenario occurs as follows: ”Alice” is a valued customer of ”Grocery store X”. ”Grocery store X” provides customers with ”loyalty card” mounted with an EPC tag. The tag serial number is combined with the customer's personal information, such as: customer's name, customer's address, date of birth, etc. ”Bob” has an RF reader and waiting out of the store to steal personal

**Program 2** WinCE Phishing proof-of-concept code.

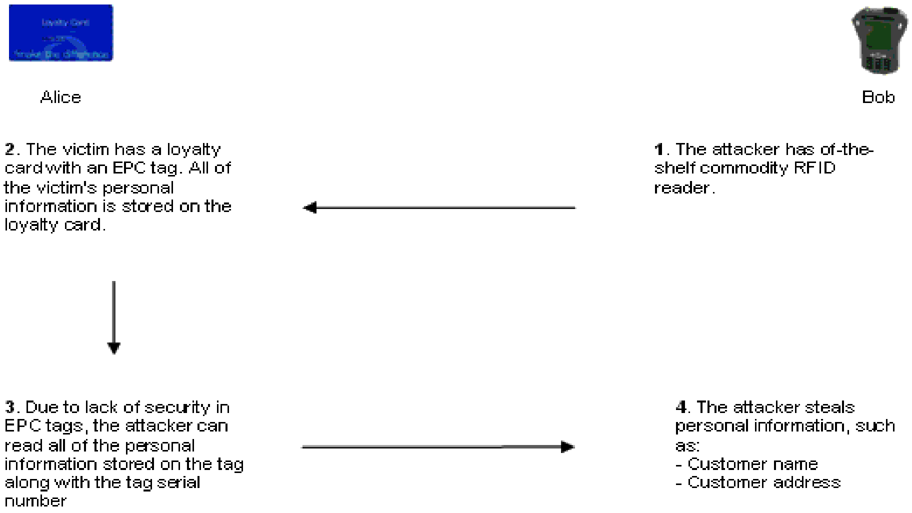
```
private void loadcontacts(){
    bool    readnext  = true;
    int     marker    = 0;
    Cursor  oldCur = Cursor.Current;
    Cursor.Current = Cursors.WaitCursor;
    listCont.Items.Clear();
    m_volume.UseSystem();
    m_table = new CeDbTable(m_volume, "Contacts Database");
    CeDbRecordSet recset = m_table.Open(CeDbOpenFlags.AutoIncrement,
                                        0x4013001F);
    listCont.BeginUpdate();
    for(readnext = true; readnext; readnext = (marker != 0)){
        CeDbRecord rec = recset.Read();
        marker = rec.Id;
        if(marker != 0){
            ContactItem item = new ContactItem(rec);
            listCont.Items.Add(item);
        }
    }
    recset.Close();
    listCont.EndUpdate();
    Cursor.Current = oldCur;
}
```

customers information. In Figure 5, we demonstrate a Phishing attack exploiting lack of security in EPC tags.

In order to highlight lack of security protection in RFID devices, Bono et al. [11] proposed a proof-of-concept attack to break cryptographic security in an RFID device known as Digital Signature Transponder (DST). They reverse-engineered DST and determined the functional details of the cipher.Thus, they were able to crack a 40 bit key with an array of sixteen FPGAs operating in parallel in under an hour using two responses to arbitrary challenges. Finally, using the key and serial number of a DST, they simulated its RF output and spoofed readers to buy gasoline at a service station and start an automobile.

## 4 Defense

There are variety of Anti-Phishing solutions in a wired-LAN. As discussed in Section 2 there are different techniques, such as: account life cycle monitors, email authentication, Phishing site takedown, brand monitors, patch and change management services, forensics and investigation, web duplication disabling, web application security, content filters, anti-malware, anti-spam, and toolbar security add-ons. However, protection in a mobile environment lacks basic anti-virus and anti-spyware solutions. Vulnerabilities are either in the architecture itself as we discussed in Wi-Fi Phishing, Bluetooth, and RFID Phishing, or in mobile applications, such as: Win CE OS and Symbian OS. There are proposed solutions to ensure security in Wi-Fi hotspots. HotSpotDK [57] is a hotspot defense kit that detects wireless attackers. HotSpotDK checks



1. The attacker has of-the-shelf commodity RFID reader.

2. The victim has a loyalty card with an EPC tag. All of the victim's personal information is stored on the loyalty card.

3. Due to lack of security in EPC tags, the attacker can read all of the personal information stored on the tag along with the tag serial number

4. The attacker steals personal information, such as:
- Customer name
- Customer address

Figure 5: RFID Phishing attack flow.

for changes in ESSID, MAC address of the access point, MAC address of the default gateway, and radical signal strength fluctuations. Should it detect a problem, HotSpotDK notifies the user that an attacker may be on the wireless network. Wireless hotspot operators should consider the following: stronger authentication mechanisms, one-time authentication setups, monitoring the existence and creation of APs. Regarding solutions for hand-held devices, Airscanner [5] has a mobile security bundle that consists of anti-virus, firewall and encrypter for Windows CE OS. However, there is no distinct cross platform anti-phishing solution dedicated to hand-held devices. In RFID there is trade off between cheap prices of RFID tags and cryptographic protection for these tags. If cheap tags need to be used in loyalty cards, grocery stores, and home appliances, lightweight cryptographic protection is needed for such devices to preserve their privacy and security.

## 5 Conclusion

The study showed that Phishing attacks can be in different forms other than forged emails and spoofed websites. Phishing attacks can occur in Wi-Fi, Bluetooth, hand-held devices, and RFID tags. In addition, we showed that Phishing attacks in a mobile environment are easier and more convincing than traditional mass mailing techniques. Although traditional Phishing attacks rely on the weakness of the recipient, Phishing in a mobile environment relies on weaknesses in the medium of transmission. Consequently, Phishing detection and take down is more difficult in such environment as it is harder to track the attacker. In Wi-Fi, setting up a rogue AP facilitates Pharming attacks and DNS poisoning. SNARF attack on Bluetooth-enabled devices enables access to restricted areas of the device. The attacker can steal personal information in the victims device, such as: contacts database, calendar, and list of received and missed calls. More dangerously, the attack can eavesdrop on phone calls, initiate phone calls, and send and receive SMS messages. We showed that it is possible to launch a Phishing attack via Bluetooth to lure victims and steal their personal information. In addition, we showed that Pocket PCs running Windows CE are vulnerable to Phishing attacks as they have equal access privileges to all users, lack strong anti-virus protection, and ease of searching registry entries. RFID tags have their own privacy and security issues. Although the public use of these tags needs more time, lightweight cryptographic schemes must be implemented to secure them. If used in loyalty cards and commercial supply chains, EPC tags are subject to inventorying and Phishing attacks as they carry personal information combined with the tag serial number.

Current defense mechanisms against Phishing attacks in a mobile environment are still inadequate. Therefore, the results motivate future work to develop new Anti-Phishing solutions in mobile environment. Future work will focus on both weaknesses in the recipient side and the transmission side. In general, future work will explore the need for anti-virus tools, anti-malware applications, and Anti-Phishing solutions for mobile applications and architectures. Till this time, Phishing attacks in a mobile environment will stay a disease that needs a cure.

## Acknowledgement

The authors would like to thank the members of APWG for providing valuable resources. In addition, the authors thank members of the MARA and Phish Track mailing lists for the fruitful discussion. The authors also would like to thank Jose Andre Morales for his help in the Windows CE contact extractor code and Nalneesh Gaur for compiling a comprehensive list of Phishing and fraud solutions.

## References

[1] Anti-Phishing Working Group. http://www.antiphishing.org.

[2] 0spam.net. http://www.0spam.net.

[3] Ben Adida, Susan Hohenberger, and Ronald L. Rivest. Fighting phishing attacks: A lightweight trust architecture for detecting spoofed emails. In *Proceedings of the DIMACS Workshop on Theft in E-Commerce*, 2005.

[4] Ben Adida, Susan Hohenberger, and Ronald L. Rivest. Separable identity-based ring signatures: Theoretical foundations for fighting phishing attacks. In *Proceedings of the DIMACS Workshop on Theft in E-Commerce*, 2005.

[5] Airscanner. http://www.airscanner.com.

[6] ID Analytics. http://www.idanalytics.com.

[7] Anonymizer. http://www.anonymizer.com.

[8] MARA: Mobile Antivirus Researchers Association. Backdoor.WinCE. http://www.mobileav.org.

[9] MARA: Mobile Antivirus Researchers Association. Pbstealer.A. http://www.mobileav.org.

[10] Bharosa. http://www.bharosa.com.

[11] Stephen C. Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel D. Rubin, and Michael Szydlo. Security analysis of a cryptographically-enabled RFID device. In *Proceedings of the 14th USENIX Security Symposium*, 2005.

[12] Brandimensions. http://www.brandimensions.com.

[13] Web Caller-ID. http://www.wholesecurity.com.

[14] ChoicePoint. www.choicepoint.com.

[15] N. Chou, R. Ledesma, Y. Teraguchi, and J.C. Mitchell. Client-side defense against web-based identity-theft. In *NDSS'04: Proceedings of Network and Distributed System Security Symposium*, 2004.

[16] Cloumark. http://www.cloumark.com.

[17] CollectiveTrust. http://www.collectivetrust.com.

[18] Corillian. http://www.corillian.com.

[19] Cyota. www.cyota.com.

[20] Cyveillance. http://www.cyveillance.com.

[21] Rachna Dhamija and J. D. Tygar. The battle against phishing: Dynamic security skins. In *SOUPS '05: Proceedings of the 2005 symposium on Usable privacy and security*, pages 77–88, New York, NY, USA, 2005. ACM Press.

[22] Andy Dornan. *The Essential Guide to Wireless Communications Applications*, pages 249–258. Prentice Hall PTR, 2nd edition, 2002.

[23] Earthlink. http://www.earthlink.net/software/free/toolbar/.

[24] Aaron Emigh. Online identity theft: Phishing technology, chokepoints and countermeasures. Radix Labs, 2005.

[25] Experian. www.experian.com.

[26] Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach. Web spoofing: An internet con game. In *Proceedings of the 20th National Information Systems Security Conference*, 1997.

[27] Fortinet. http://www.fortinet.com.

[28] Simson Garfinkel and Beth Rosenberg. *RFID : Applications, Security, and Privacy*. Addison-Wesley, 2005.

[29] Brad Grimes. Will Wal-Mart Track You? PC World. http://msn.pcworld.com/news/article/0,aid,115139,00.asp.

[30] Anti-Phishing Working Group. Phishing activity trends report, November, 2005.

[31] Dell'Oro Group. http://www.delloro.com/.

[32] Martin Herfurt. Detecting and attacking bluetooth-enabled cellphones at the hannover fairground. In *CeBIT 2004*, 2004.

[33] Amir Herzberg and Ahmad Gbara. Trustbar: Protecting (even nave) web users from spoofing and phishing attacks. Cryptology ePrint Archive, Report 2004/155, 2004. http://eprint.iacr.org/.

[34] Internet Identity. http://www.internetidentity.com.

[35] Markus Jakobsson. Modeling and preventing phishing attacks. In *Financial Cryptography*, 2005.

[36] Markus Jakobsson and Adam Young. Distributed phishing attacks. Cryptology ePrint Archive, Report 2005/091, 2005.

[37] Lance James. *Phishing Exposed*. Syngress, 2005.

[38] JiWire. http://www.jiwire.com/.

[39] Ari Juels. RFID security and privacy: A research survey. *to appear in IEEE Journal on Selected Areas in Communication*, 2006.

[40] Ben Laurie and Adam Laurie. Serious flaws in bluetooth security lead to disclosure of personal data. Technical report, A.L. Digital Ltd., 2004. http://bluestumbler.org.

[41] LexisNexis. http://www.lexisnexis.com.

[42] MarkMonitor. http://www.markmonitor.com.

[43] Microsoft. http://www.microsoft.com/mscorp/safety/technologies/antiphishing/default.mspx.

[44] Daisuke Miyamoto, Hiroaki Hazeyama, and Youki Kadobayashi. SPS: A simple filtering algorithm to thwart phishing attacks. In *AINTEC*, pages 195–209, 2005.

[45] Jose Andre Morales, Peter J. Clarke, and Yi Deng. Testing and evaluation of virus detectors for handheld devices. In *Proceedings of NIST Workshop on Software Security Assurance Tools, Techniques, and Metrics (SSATTM)*, 2004.

[46] NameProtect. http://www.nameprotect.com.

[47] Netcraft. http://toolbar.netcraft.com/.

[48] Ethereal: A Network Protocol Analyzer. http://www.ethereal.com/.

[49] Phil Nobles and Peter A Horrocks. Vulnerability of IEEE802.11 WLANs to MAC layer DoS attacks. In *Proceedings of the 2nd IEE Secure Mobile Communications Forum*, 2004.

[50] Philip Nobles. Security and the convergence of wireless standards. presented at ETSI Future Security Workshop: The threats, risks and opportunities, January 2006. Sophia Antipolis, France.

[51] Gunter Ollmann. The phishing guide: Understanding and preventing phishing attacks. NGS Software Insight Security Research, 2004.

[52] America Online and the National Cyber Security Alliance. AOL/NCSA Online Safety Study, December 2005.

[53] F-Secure Virus Descriptions : Pbstealer.A. http://www.f-secure.com/v-descs/pbstealer_a.shtml.

[54] Primedius. http://www.primedius.com.

[55] Qsent. http://www.qsent.com.

[56] Srivaths Ravi, Anand Raghunathan, Paul Kocher, and Sunil Hattangady. Security in embedded systems: Design challenges. *Trans. on Embedded Computing Sys.*, 3(3):461–491, 2004.

[57] Airsnarf: A rogue AP setup utility. http://airsnarf.shmoo.com/.

[58] Secure Science. http://www.securescience.com.

[59] A. Shamara, M. Topkara, M. Atallah, and C. Nita-Rotaru. WiViD: Visible watermak based defense against phishing. In *IWDW '05: Proceedings of the International Workshop of Digital Watermarking*, 2005.

[60] Bluetooth SIG. Bluetooth specifications 1.0, 1.1, 1.2 and 2.0+EDR. http://www.bluetooth.org.

[61] Bluetooth SIG. Bluetooth Annual Report, 2004.

[62] SpoofStick. http://www.spoofstick.com.

[63] TippingPoint. http://www.tippingpoint.com.

[64] The trifinite.group. Blooover. http://trifinite.org.

[65] The trifinite.group. Bluebug. http://trifinite.org.

[66] TrustWatch. http://www.trustwatch.com.

[67] Verisign. http://www.verisign.com.

[68] Liu Wenyin, Guanglin Huang, Liu Xiaoyue, Zhang Min, and Xiaotie Deng. Detection of phishing webpages based on visual similarity. In *WWW '05: Special interest tracks and posters of the 14th international conference on World Wide Web*, pages 1060–1061, New York, NY, USA, 2005. ACM Press.

[69] KARMA Wireless Client Security Assessment Tools. http://www.theta44.org/karma/.

[70] Min Wu, Rob Miller, and Simon Garfinkel. Do security toolbars actually prevent phishing attack? In *SOUPS 2005: Proceedings of Symposium On Usable Privacy and Security (poster)*, 2005.

[71] D. Dai Zovi and S. Macaulay. Attacking automatic wireless network selection. In *Proceedings of the 6th IEEE Information Assurance Workshop*, 2005.