SECURITY IN COMPUTING, FIFTH EDITION

Chapter 4: The Web—User Side

Module 3 Web Attacks

- Attacks against browsers
- Attacks against and from web sites
- Attacks seeking sensitive data
- Attacks through email

Browser attacks

Browser is software with a relatively simple role:

- connect to a particular web address
- fetch and display content from that address
- transmit data from a user to that address

Security issues for browsers arise from several complications such as

- A browser often connects to more than the one address shown in the browser's address bar.
- Fetching data can impose accesses to numerous locations to obtain pictures, audio content, and other linked content.

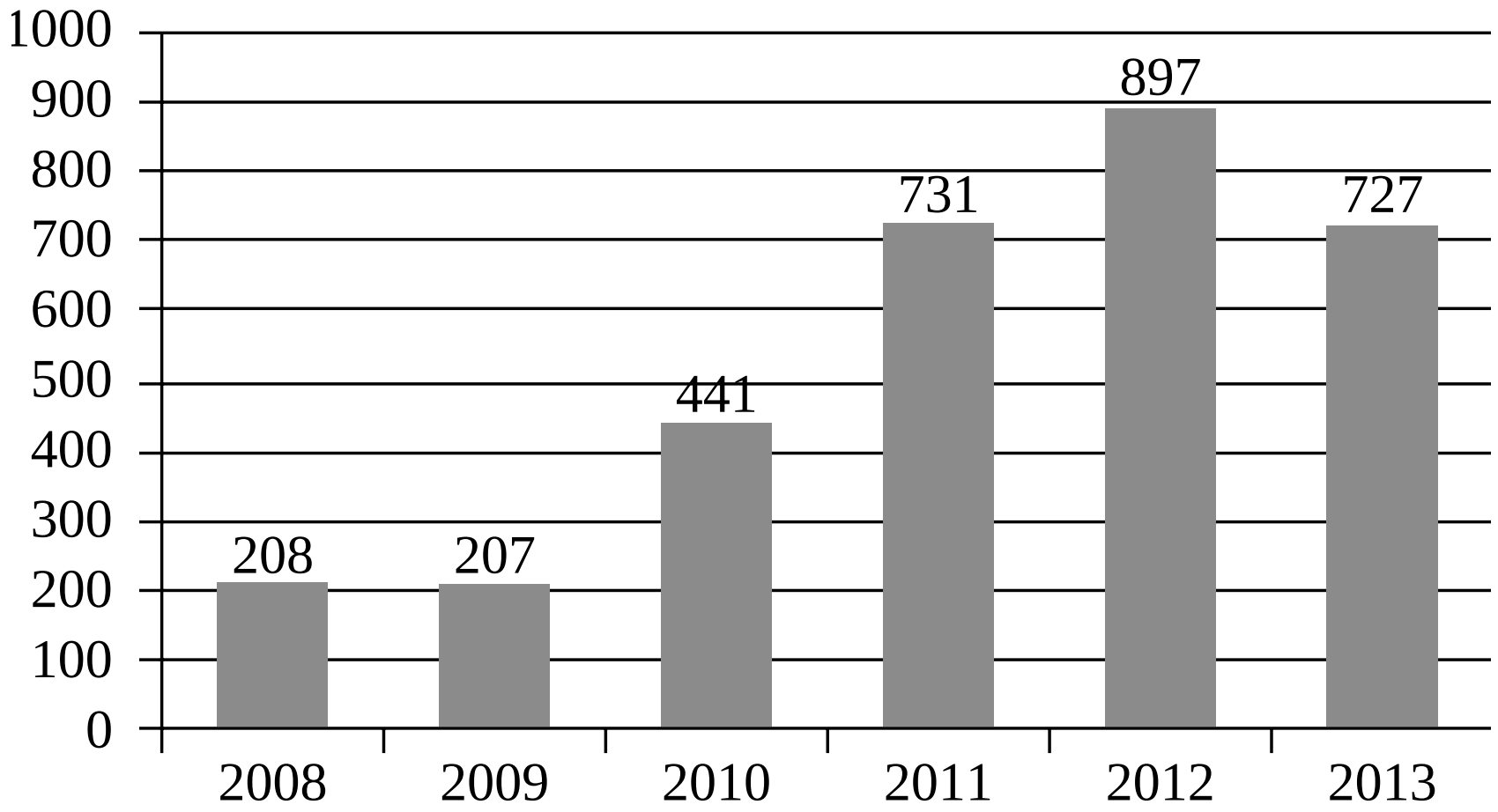
Browser attacks

- Browser software can be malicious or can be corrupted to acquire malicious functionality.
- Popular browsers support add-ins, extra code to add new features to the browser, but these add-ins themselves can include corrupting code.
- Data display involves a rich command set that controls rendering, positioning, motion, layering, and even invisibility.
- The browser can access any data on a user's computer (subject to access control restrictions); generally the browser runs with the same privileges as the user.
- Data transfers to and from the user are invisible, meaning they occur without the user's knowledge or explicit permission.

Browser attacks

- Browsers connect users to outside networks, but few users can monitor the actual data transmitted
- Many web interactions start at site A but then connect automatically to sites B, C, and D, often without the user's knowledge, much less permission, once data arrive at site A, the user has no control over what A does.
- Ways to attack browser
- Go after the operating system so it will impede the browser's correct and secure functioning.
- Tackle the browser or one of its components, add-ons, or plug-ins so its activity is altered.
- Intercept or modify communication to or from the browser.

Browser Vulnerabilities



Browser Attack Types

- Man-in-the-browser
- Keystroke logger
- Page-in-the-middle
- Program download substitution
- User-in-the-middle

Man-in-the-Browser

- A man-in-the-browser attack is an example of malicious code that has infected a browser.
- Code inserted into the browser can read, copy, and redistribute anything the user enters in a browser.
- The threat here is that the attacker will intercept and reuse credentials to access financial accounts and other sensitive data.
- Trojan horse that intercepts data passing through the browser

Man-in-the-Browser

User types

Browser encrypts

Encrypted data transferred to bank

SilentBanker intercepts

Man-in-the-Browser

- Code linked to a victim's browser as an add-on or browser helper object; in some versions it listed itself as a plug-in to display video. As a helper object,
- It set itself to intercept internal browser calls, including those to receive data from the keyboard, send data to a URL, generate or import a cryptographic key, read a file (including display that file on the screen), or connect to a site;
- SilentBanker started with a list of over 400 URLs of popular banks throughout the world.
- Whenever it saw a user going to one of those sites, it redirected the user's keystrokes through the Trojan horse and recorded customer details that it forwarded to remote computers (presumably controlled by the code's creators).

Keystroke Logger

- Hardware or software that records all keystrokes
- May be a small dongle plugged into a USB port or can masquerade as a keyboard
- May also be installed as malware
- In software, the logger is just a program installed like any malicious code. Such devices can capture passwords, login identities, and all other data typed on the keyboard.
- Although not limited to browser interactions, a keystroke logger could certainly record all keyboard input to the browser

Page-in-the-Middle

- User is directed to a different page than believed or intended
- when the user clicks “login” to go to the login page of any site, the attack might redirect the user to the attacker’s page, where the attacker can also capture the user’s credentials.
- Similar effect to a man-in-the-browser, where attacker can intercept and modify user input

Program Download Substitution

- Attacker creates a page with seemingly innocuous and desirable programs for download
- Instead of, or in addition to, the intended functionality, the user installs malware
- This is a very common technique for spyware
- A user agreeing to install a program has no way to know what that program will actually do.

User-in-the-Middle

- Using click-bait to trick users into solving CAPTCHAs on spammers' behalf
- The attacker in the middle splices together two interactions by inserting a small amount of the account creation thread into the middle of the photo access thread.
- The user is unaware of the interaction in the middle.

Successful Authentication

- The attacks are largely failures of authentication
- Common examples of these mechanisms are SecurID tokens, Google Authenticator, and text message codes. Driver signing is an example of using such techniques to mitigate local malware.
- Can be mitigated with
  - Shared secret
  - One-time password
  - Out-of-band communication

Shared secret

- The basic concept is of a shared secret, something only the two entities on the end should know.
- A human man-in-the-middle attack can be defeated if one party asks the other a pointed question about a dinner they had together or details of a recent corporate event, or some other common topic.
- Similarly, a shared secret for computer systems can help authenticate.
- Possible secrets could involve the time or date of last login, time of last update, or size of a particular application file.
- To be effective, a shared secret must be something no malicious middle agent can know.

One-time password

- one-time password is good for only one use.
- To use a one-time password scheme, the two end parties need to have a shared secret list of passwords.
- When one password is used, both parties mark the word off the list and use the next word the next time.
- The SecurID token, generates a new random number every 60 seconds.
- The receiving computer has a program that can compute the random number for any given moment, so it can compare the value entered against the expected value.

Out-of-band communication

- Out-of-band communication means transferring one fact along a communication path separate from that of another fact.
- If a customer calls a bank about having forgotten a PIN, the bank does not simply provide a new PIN in that conversation over the phone; the bank mails a separate letter containing a new PIN to the account-holder's address on file.
- In this way, if someone were impersonating the customer, the PIN would not go to the impersonator.
- Some banks confirm large Internet fund transfers by sending a text message to the user's mobile phone.

Web Attacks Targeting Users

- Two classes of situations involving web content.
- The first kind involves false content, most likely because the content was modified by someone unauthorized; with these the intent is to mislead the viewer.
- The second, more dangerous, kind seeks to harm the viewer.

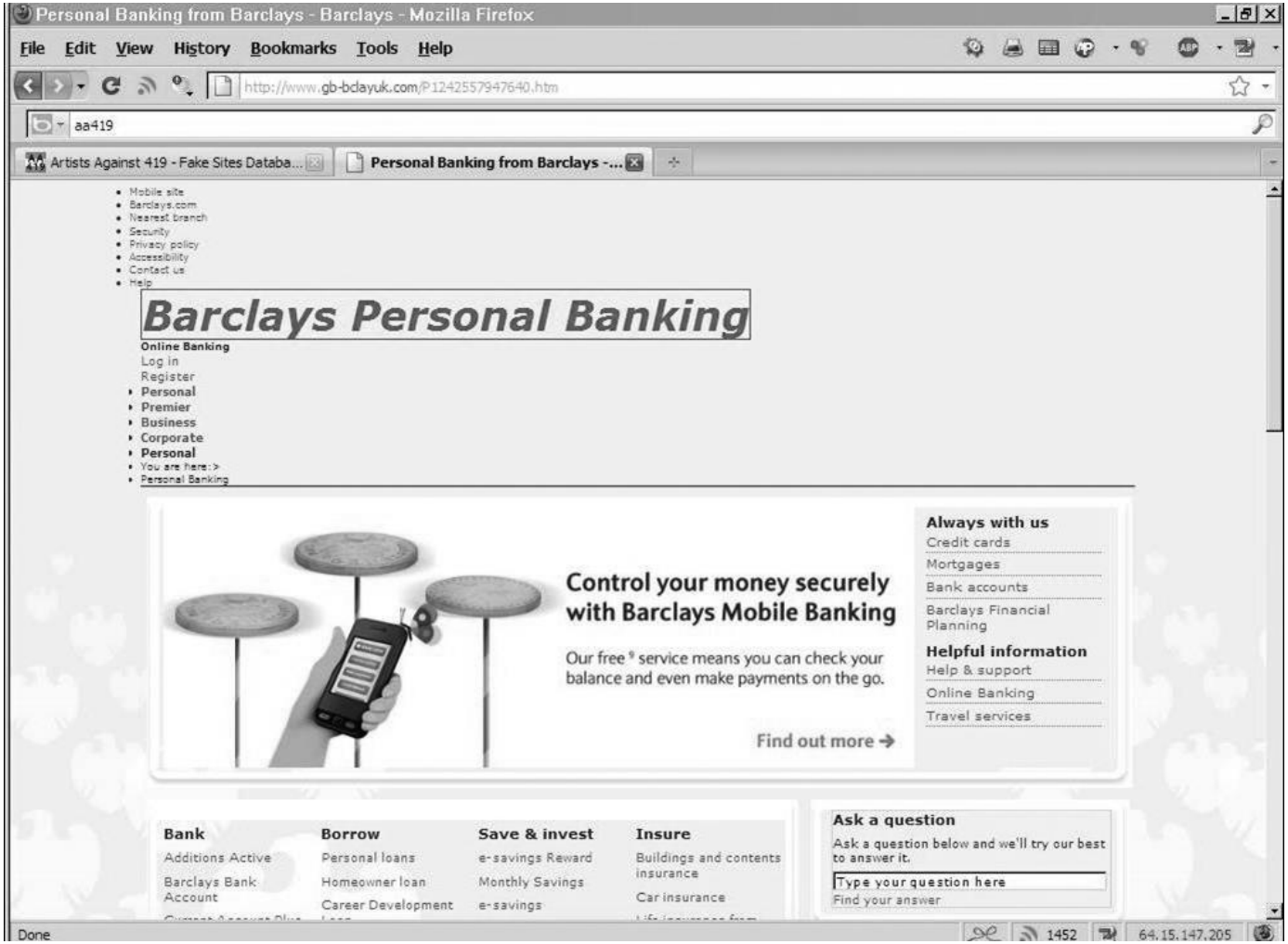
Defaced Web Site

- website defacement occurs when an attacker replaces or modifies the content of a legitimate web site.
- The objectives of website defacements also vary.
- Sometimes the goal is just to prove a point or embarrass the victim.

Fake Web Site

- Web sites are easy to fake because the attacker can obtain copies of the images the real site uses to generate its web site.
- All the attacker has to do is change the values of links to redirect the unsuspecting victim to points of the attacker's choosing.
- The attacker can get all the images a real site uses; fake sites can look convincing.

Fake Website



Fake Code

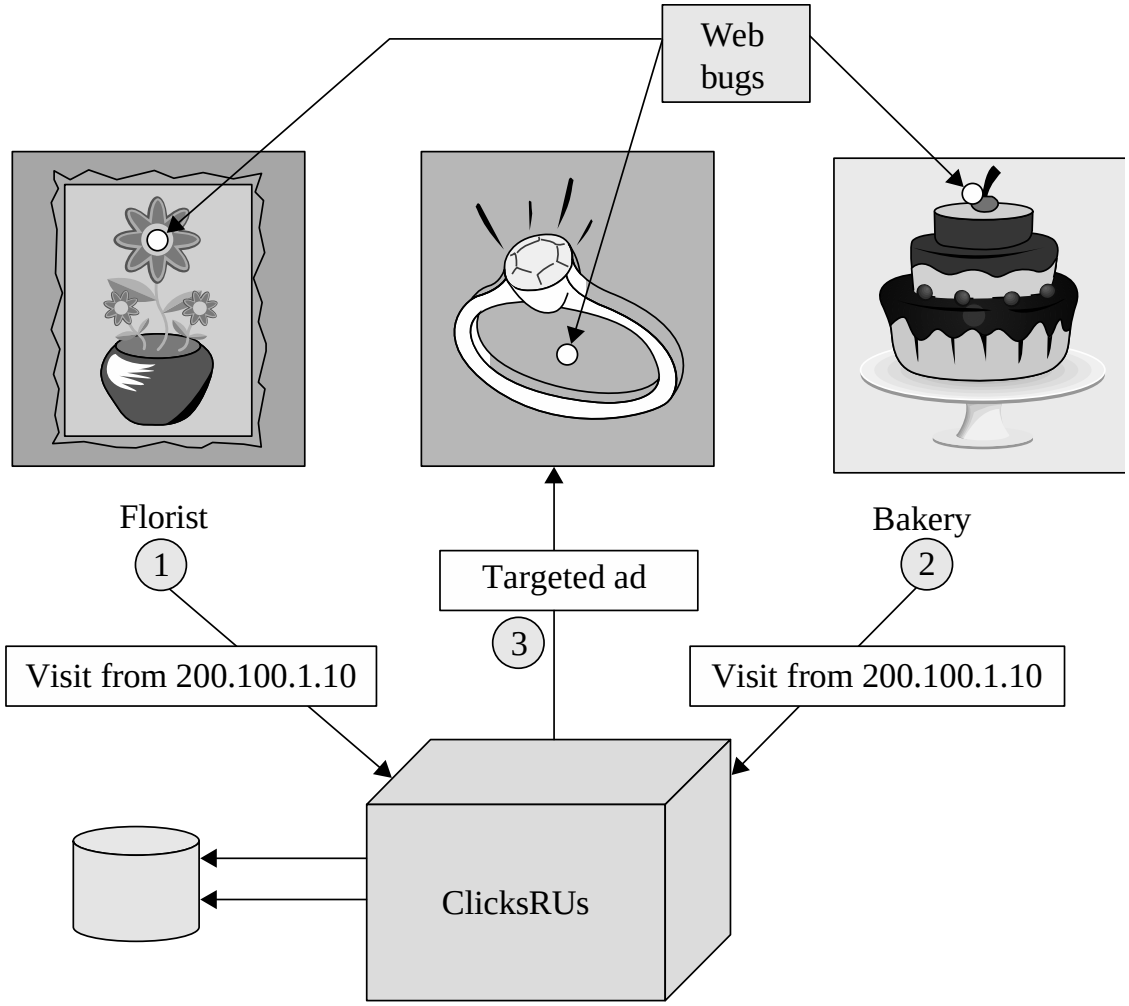
Tracking Bug

- Some advertisers want to count number of visitors and number of times each visitor arrives at a site.
- They can do this by a combination of cookies and an invisible image.
- A web bug, also called a clear GIF, 1x1 GIF, or tracking bug, is a tiny image, as small as 1 pixel by 1 pixel (depending on resolution, screens display at least 100 to 200 pixels per inch), an image so small it will not normally be seen.
- It is loaded and processed the same as a larger picture. Part of the processing is to notify the bug's owner,
- The advertiser, who thus learns that another user has loaded the advertising image.

Tracking Bug

- A single company can do the same thing without the need for a web bug.
- If you order flowers online, the florist can obtain your IP address and set a cookie containing your details so as to recognize you as a repeat customer.
- A web bug allows this tracking across multiple merchants.

Tracking Bug



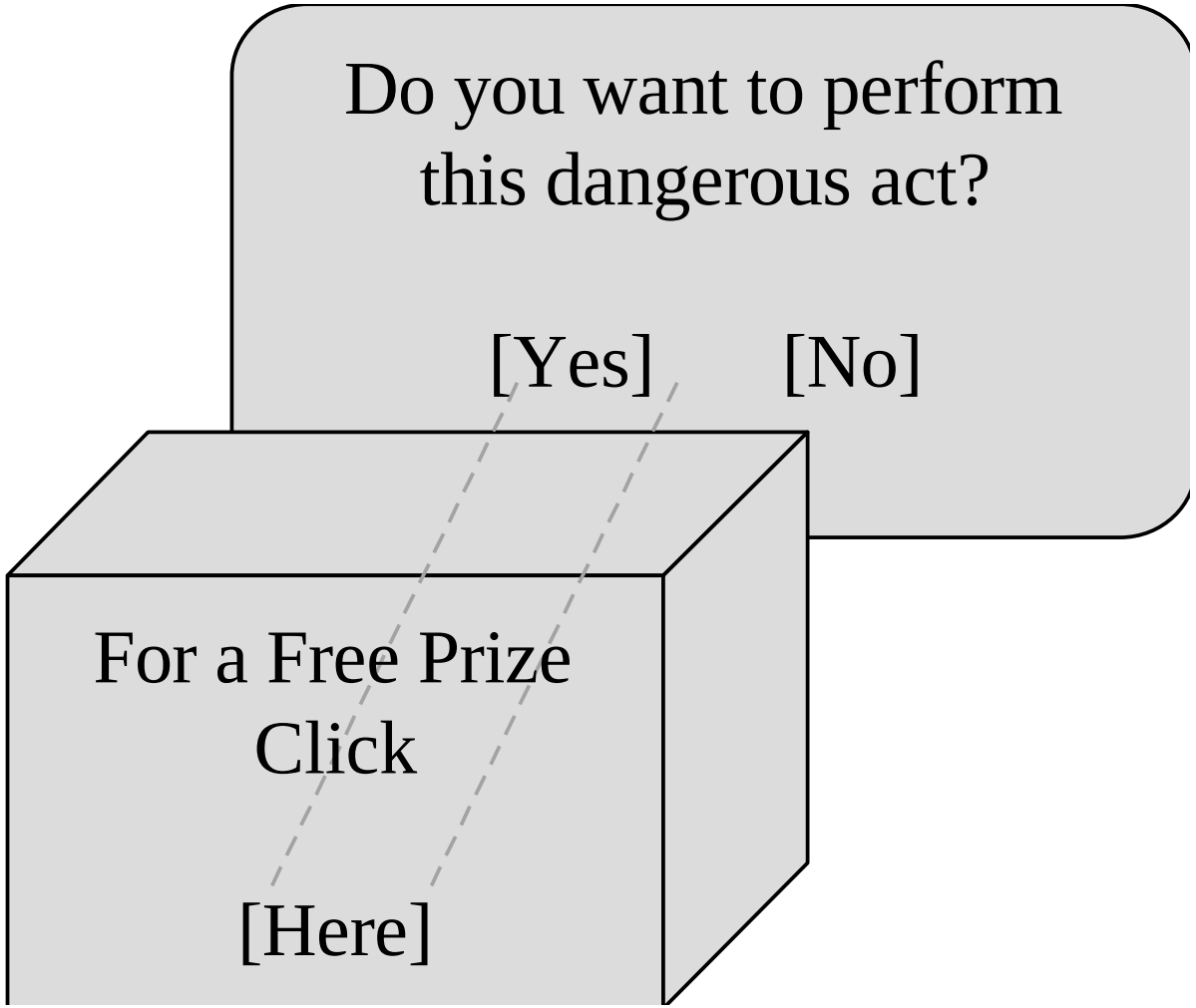
Tracking Bug

- Florist might subscribe to a web tracking service, which we name ClicksRUs.
- The florist includes a web bug in its web image, so when you load that page, your details are sent to ClicksRUs, which then installs a cookie.
- If you leave the florist's web site and next go to a bakery's site that also subscribes to tracking with ClicksRUs, the new page will also have a ClicksRUs web bug.
- This time,, ClicksRUs retrieves its old cookie, finds that you were last at the florist's site, and records the coincidence of these two firms. After correlating these data points

Tracking Bug

- ClicksRUs can inform the florist and the bakery that they have common customers and might develop a joint marketing approach.
- Or ClicksRUs can determine that you went from florist A to florist B to florist C and back to florist A, so it can report to them that B and C lost out to A, helping them all develop more successful marketing strategies.
- Or ClicksRUs can infer that you are looking for a gift and will offer a targeted ad on the next site you visit.
- ClicksRUs might receive advertising revenue from florist D and trinket merchant E, which would influence the ads it will display to you.

Clickjacking



Clickjacking

- Clickjacking: Tricking a user into clicking a link by disguising what the link points to.
- A clickjacking attack succeeds because of what the attacker can do:
- choose and load a page with a confirmation box that commits the user to an action with one or a small number of mouse clicks (for example, “Do you want
- to install this program? [Yes] [Cancel]”)
- • change the image’s coloring to transparent
- • move the image to any position on the screen

Clickjacking

- The two technical tasks, changing the color to transparent and moving the page, are both possible because of a technique called framing, or using an iframe.
- An iframe is a structure that can contain all or part of a page, can be placed and moved anywhere on another page, and can be layered on top of or underneath other frames.

Drive-By Download

- Code is downloaded, installed, and executed on a computer without the user's knowledge
- May be the result of clickjacking, fake code, program download subsitution, etc.

Drive-By Download

- Downloading and installing code other than what a user expects

Among the changes he detected were

- eight new programs from at least four different companies
- nine new directories
- three new browser toolbars (including the interesting toolbar
- numerous new desktop icons
- an addition to the bottom of the Save As dialog box, offering the opportunity to buy a computer accessory and take part in a survey to enter a sweepstakes
- numerous new Favorites entries
- a new browser start page

Obtaining User or Website Data

- Someone interested in obtaining unauthorized data from the background database server crafts and passes SQL commands to the server through the web interface. Similar attacks involve writing scripts in Java.
- These attacks are called scripting or injection attacks because the unauthorized request is delivered as a script or injected into the dialog with the server.

Cross-Site Scripting (XSS)

- Executable code is included in the interaction between client and server and executed by the client or server. consider a simple command to the search engine Google. The user enters a simple text query,
- but handlers add commands along the way to the server, so what starts as a simple string becomes a structure that Google can use to interpret or refine the search, or that the user's browser can use to help display the results.
- So, for example, a Google search on the string "cross site scripting" becomes

```
http://www.google.com/search?q=cross+site+scripting
&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official
&client=firefox-a&lr=lang_en
```

Cross-Site Scripting (XSS)

- Sometimes,, the interaction is not directly between the user's browser and one web site.
- Many web sites offer access to outside services without leaving the site. For example, television station KCTV in Kansas City has a website with a search engine box so that a user can search within the site or on the web. In this case, the Google search result is displayed within a KCTV web page a convenience to the user and a marketing advantage for KCTV (because the station keeps the user on its web site).
- The search query is loaded with parameters to help KCTV display the results; Google interprets the parameters for it and returns the remaining parameters unread and unmodified in the result to KCTV.
- These parameters become a script attached to the query and executed by any responding party along the way.

Cross-Site Scripting (XSS)

- Tricking a client or server into executing scripted code by including the code in data inputs
- Scripts and HTML tags are encoded as plaintext just like user inputs, so they can take over web pages similarly to the way buffer overflow attacks can take over programs

```
Cool<br>story.<br>KCTVBigFan<script
src=http://badsite.com/xss.js></script>
```

SQL Injection

- Injecting SQL code into an exchange between an application and its database server
- Example:
  - Loading an SQL query into a variable, taking the value of acctNum from an arbitrary user input field:
  - `QUERY = "SELECT * FROM trans WHERE acct = '" + acctNum + " '; "`
  - The same query with malicious user input:
  - `QUERY = "SELECT * FROM trans WHERE acct = '2468' OR '1'='1'; "`

Dot-Dot-Slash

- Also known as “directory traversal,” this is when attackers use the term “../” to access files that are on the target web server but not meant to be accessed from outside
- Most commonly entered into the URL bar but may also be combined with other attacks, such as XSS

```
http://yoursite.com/webhits.htw?CiWebHits&File=../../../../../winnt/system32/autoexec.nt
```

Server-Side Include (SSI)

- SSI is an interpreted server-side scripting language that can be used for basic web server directives, such as including files and executing commands
- As is the case with XSS, some websites are vulnerable to allowing users to execute SSI directives through text input

```
<!--#exec cmd="/usr/bin/telnet &"-->
```

Countermeasures to Injections

- Filter and sanitize all user input
  - Need to account for every potentially valid encoding
- Make no assumptions about the range of possible user inputs—trust nothing, check everything
- Use access control mechanisms on backend servers, such as “stored procedures”

Email Attacks

- An attacker can attempt to fool people with fake email messages.
- Spam, fictitious or misleading email, offers to buy designer watches, or hot stocks, as well as get-rich schemes involving money in overseas bank accounts.
- Similar false messages try to get people to click to download a browser enhancement or even just click for more detail.
- Spammers now use more realistic topics for false messages to entice recipients to follow a malicious link
- Eg. current events messages (“Want more details on [sporting event, political race,crisis]?”)

Email Spam

- Experts estimate that 60% to 90% of all email is spam
- Types of spam:
  - Advertising
    - Pharmaceuticals
    - Stocks
  - Malicious code
  - Links for malicious websites
- Spam countermeasures
  - Laws against spam exist but are generally ineffective
  - Email filters have become very effective for most spam
  - Internet service providers use volume limitations to make spammers' jobs more difficult

Phishing

- **Phishing** – Cybercriminal attempts to steal personal and financial information or infect computers and other devices with malware and viruses
  - Designed to trick you into clicking a link or providing personal or financial information
  - Often in the form of emails and websites
  - May appear to come from legitimate companies, organizations or known individuals
  - Take advantage of natural disasters, epidemics, health scares, political elections or timely events

Phishing

Different forms such as:

- **Mass Phishing** – Mass, large-volume attack intended to reach as many people as possible
- **Whaling** – Type of spear phishing attack that targets “big fish,” including high-profile individuals or those with a great deal of authority or access
- **Clone Phishing** – Spoofed copy of a legitimate and previously delivered email, with original attachments or hyperlinks replaced with malicious versions, which is sent from a forged email address so it appears to come from the original sender or another legitimate source
- **Advance-Fee Scam:** Requests the target to send money or bank account information to the cybercriminal
- And **Spear Phishing…..**

Spear Phishing

- Spear phishing is on the rise because it works. Traditional security defences do not detect and stop it.
- From a cyber criminal's point of view, spear phishing is the perfect vehicle for a broad array of damaging exploits.
- Threat actors are increasingly targeting executives and other high-level employees, tricking them into activating malware that gives criminals access into their companies' environments.
- This might be ransomware that encrypts company data, then extorts fees from the victim to remediate the situation.
- Targeted executives are usually key leaders with titles such as chief financial officer, head of finance, senior vice president and director.

Spear Phishing

- Spear phishing emails tend to have enough detail to fool even experienced security professionals.
- A phishing campaign may blanket an entire database of email addresses, but spear phishing targets specific individuals within specific organizations with a specific mission.
- By mining social networks for personal information, an attacker can write emails that are extremely accurate and compelling.
- Once the target clicks on a link or opens an attachment, the attacker establishes a foothold in the network, enabling them to complete their illicit mission.
- 84% of organizations said a spear-phishing attack successfully penetrated their organization in 2015

Common Baiting Tactics

- **Notification from a help desk or system administrator**
  Asks you to take action to resolve an issue with your account (e.g., email account has reached its storage limit), which often includes clicking on a link and providing requested information.

- **Advertisement for immediate weight loss, hair growth or fitness prowess**
  Serves as a ploy to get you to click on a link that will infect your computer or mobile device with malware or viruses.

Common Baiting Tactics

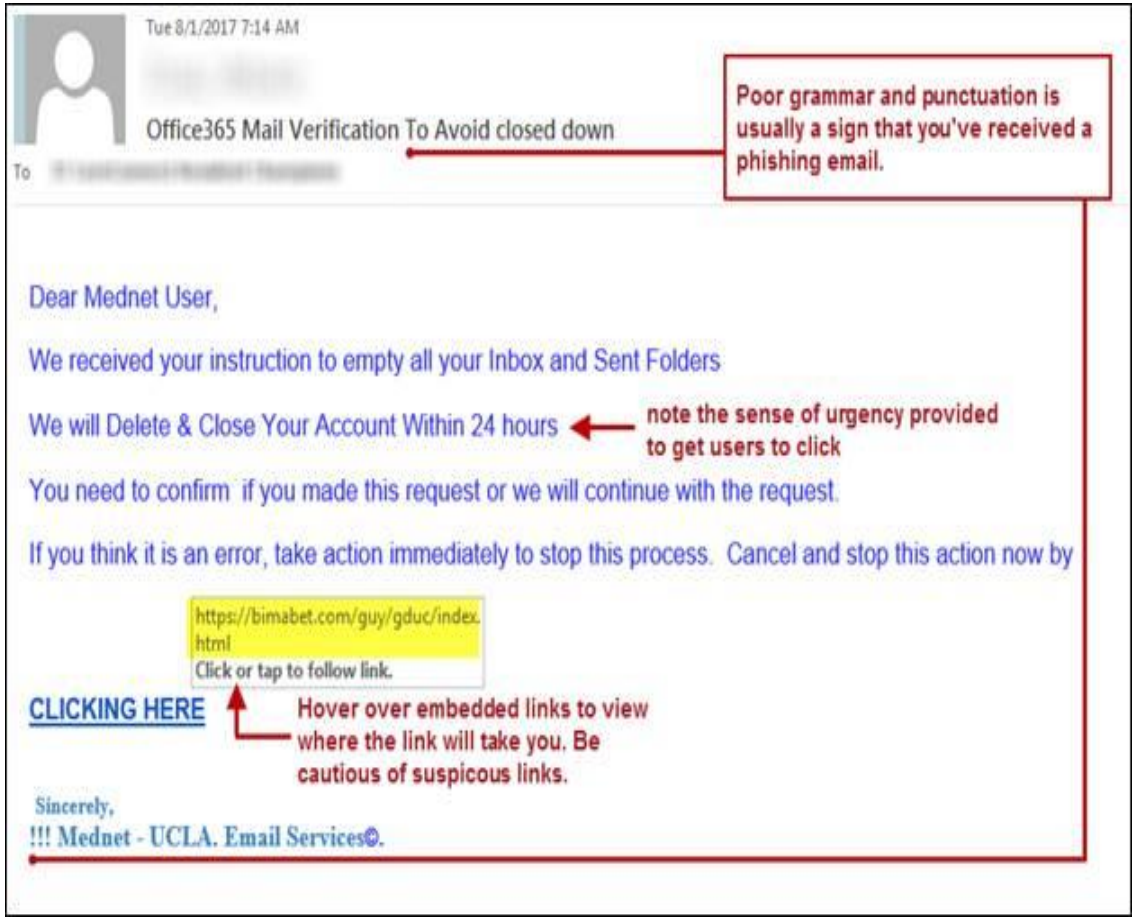
- **Attachment labeled “invoice” or “shipping order”**
  Contains malware that can infect your computer or mobile device if opened. May contain what is known as “ransomware,” a type of malware that will delete all files unless you pay a specified sum of money.

- **Notification from what appears to be a credit card company**
  Indicates someone has made an unauthorized transaction on your account. If you click the link to log in to verify the transaction, your username and password are collected by the scammer.

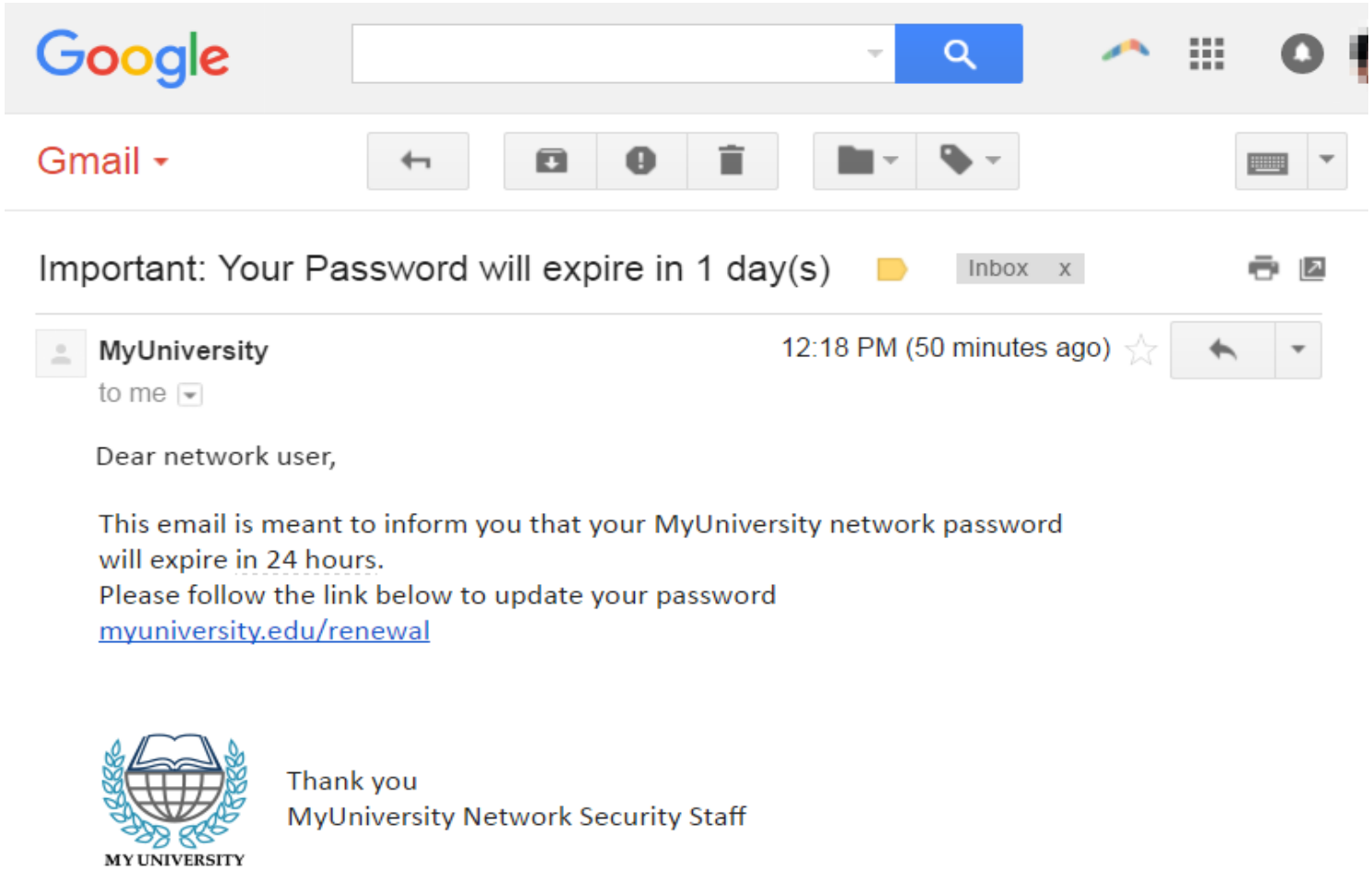
- **Fake account on a social media site**
  Mimics a legitimate person, business or organization. May also appear in the form of an online game, quiz or survey designed to collect information from your account.

Phishing Lure

- Often makes it look like a problem with one of your accounts
  - Or they try to takes advantage of an ongoing humanitarian crisis



Can you detect a phishing scam?



Google

Gmail

Important: Your Password will expire in 1 day(s) Inbox x

MyUniversity 12:18 PM (50 minutes ago)

to me

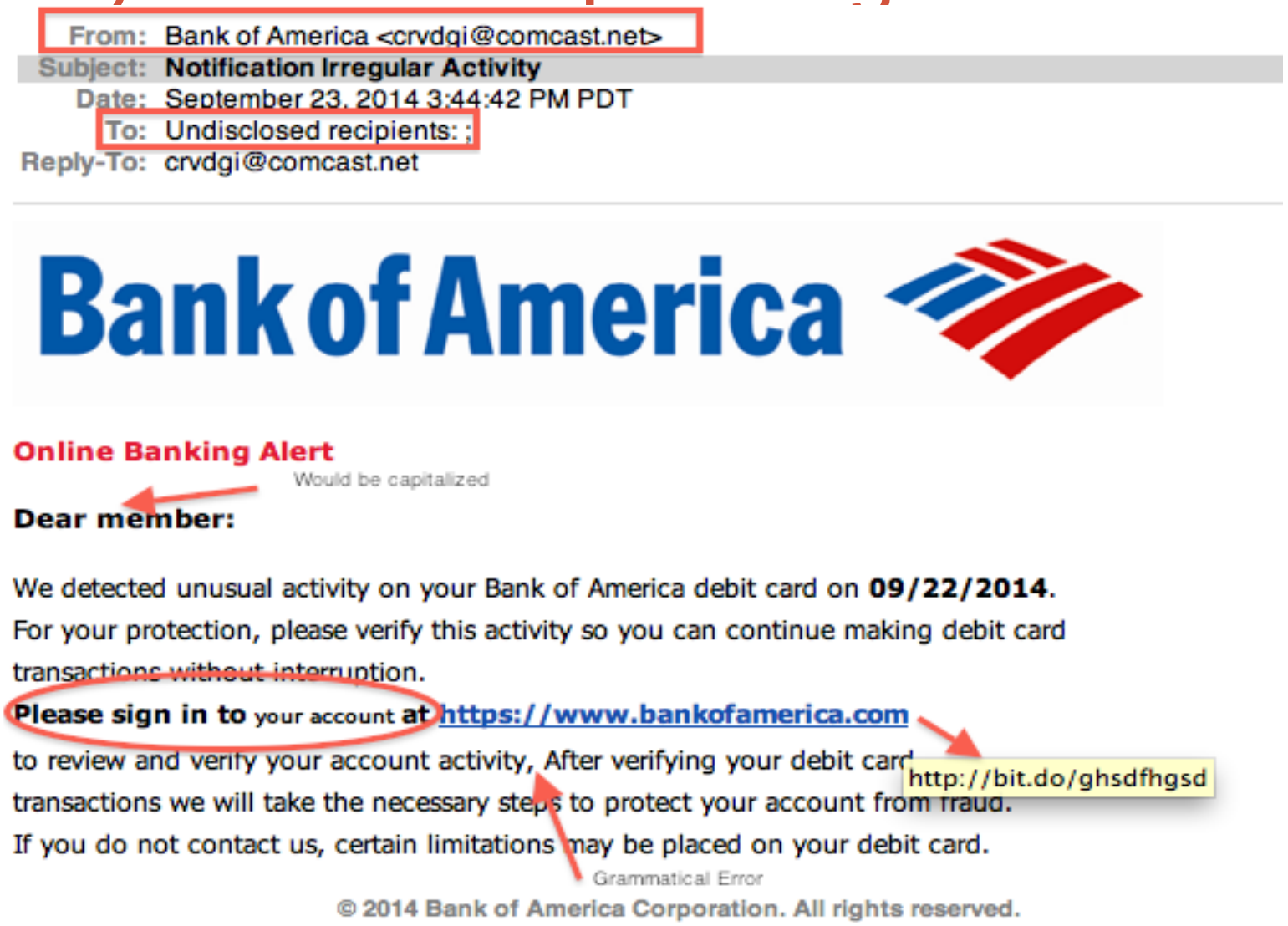
Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

MY UNIVERSITY

Thank you
MyUniversity Network Security Staff

Can you detect a phishing scam?



From: Bank of America <crvdgi@comcast.net>
Subject: **Notification Irregular Activity**
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients: ;
Reply-To: crvdgi@comcast.net

Bank of America

Online Banking Alert

Would be capitalized

Dear member:

We detected unusual activity on your Bank of America debit card on **09/22/2014**.
For your protection, please verify this activity so you can continue making debit card transactions without interruption.
Please sign in to your account **at** https://www.bankofamerica.com
to review and verify your account activity, After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.
If you do not contact us, certain limitations may be placed on your debit card.

http://bit.do/ghsdfhgsd

Grammatical Error

Common phishing scam Subject Lines

Barracuda Networks researchers compiled a list of the top 12 most common subject lines used in phishing emails targeting businesses.

Researchers analyzed over 360,000 phishing emails & found the most common subject line used in attacks is simply ‘Request’ – accounting for over a third of all the phishing messages analyzed.

The report found the top 12 subject lines were as followed:

1. Request
2. Follow up
3. Urgent/Important
4. Are you available?/Are you at your desk?
5. Payment Status
6. Hello
7. Purchase
8. Invoice Due
9. Re:
10. Direct Deposit
11. Expenses
12. Payroll

Spear Phishing Characteristics

A spear-phishing attack can display one or more of the following characteristics:

• Blended or multi-vector threat. Spear phishing uses a blend of email spoofing, dynamic URLs and drive-by downloads to bypass traditional defenses.

• Use of zero-day vulnerabilities. Advanced spear-phishing attacks leverage zero-day vulnerabilities in browsers, plug-ins and desktop applications to compromise systems.

• Multi-stage attack. The initial exploit of systems is the first stage of an APT attack that involves further stages of malware outbound communications, binary downloads and data exfiltration.

• Well-crafted email forgeries: Spearphishing email threats are usually targeted to individuals, so they don’t bear much resemblance to the high-volume, broadcast spam that floods the Internet. This means traditional reputation and spam filters routinely miss these messages, rendering traditional email protections ineffective.

How to protect against phishing

- STOP. THINK. CONNECT.
  - Before you click, look for common baiting tactics e.g. Requests for personal information, Announcement indicating you won a prize or lottery or Requests for donations
  - Look for spelling errors (e.g., “pessward”), lack of punctuation or poor grammar
  - Hyperlinked URL differs from the one displayed, or it is hidden
  - Threatening language that calls for immediate action
- Install and maintain antivirus software on your electronic devices
- Use email filters to reduce spam and malicious traffic

How to protect against phishing

- Be wary of messages asking for passwords or other personal information
  - All reputable businesses and organizations will never ask for your password via email
- Never send passwords, bank account numbers or other private information in an email
  - Do not reply to requests for this information
  - Verify by contacting the company or individual, but do not use the contact information included in the message

How to protect against phishing

- Do not click on any hyperlinks in the email
  - User your computer mouse to hover over each link to verify its actual destination, even if the message appears to be from a trusted source
  - Pay attention to the URL and look for a variation in spelling or different domain (e.g., ulster.ac vs. ulster.com)
  - Consider navigating to familiar sites on your own instead of using links within messages

- Examine websites closely
  - Malicious websites may look identical to legitimate sites
  - Look for “https://” or a lock icon in the address bar before entering any sensitive information on a website

Protecting Against Email Attacks

not to trust the content of email from a malicious or unknown sender, and source email addresses can be spoofed so any message can appear to come from a trusted source.

need a way to ensure the authenticity of email from supposedly reliable sources.

PGP

PGP stands for Pretty Good Privacy. It was invented by Phil Zimmerman in 1991.

Originally a free package, it became a commercial product after being bought by Network Associates in 1996.

A freeware version is still available. PGP is widely available, both in commercial versions and freeware.

Protecting Against Email Attacks

PGP addresses the key distribution problem with what is called a “ring of trust” or a user’s “keyring.”

One user directly gives a public key to another, or the second user fetches the first’s public key from a server.

Some people include their PGP public keys at the bottom of email messages. And one person can give a second person’s key to a third (and a fourth, and so on).

Thus, the key association problem becomes one of caveat emptor (let the buyer beware): If I trust you, I may also trust the keys you give me for other people.

The model breaks down intellectually when you give me all the keys you received from people, who in turn gave you all the keys they got from still other people, who gave them all their keys,and so forth.

Protecting Against Email Attacks

- Create a random session key for a symmetric algorithm.
- Encrypt the message, using the session key (for message confidentiality).
- Encrypt the session key under the recipient's public key.
- Generate a message digest or hash of the message; sign the hash by encrypting it with the sender's private key (for message integrity and authenticity).
- Attach the encrypted session key to the encrypted message and digest.
- Transmit the message to the recipient.

The recipient reverses these steps to retrieve and validate the message content.

Protecting Against Email Attacks

•S/MIME

An Internet standard governs how email is sent and received. The general MIME specification defines the format and handling of email attachments.

S/MIME (Secure Multipurpose Internet Mail Extensions) is the Internet standard for secure email attachments.

The principal difference between S/MIME and PGP is the method of key exchange.

Basic PGP depends on each user's exchanging keys with all potential recipients and establishing a ring of trusted recipients;

It also requires establishing a degree of trust in the authenticity of the keys for those recipients.

Protecting Against Email Attacks

- S/MIME uses hierarchically validated certificates, usually represented in X.509 format, for key exchange.

Thus, with S/MIME, the sender and recipient do not need to have exchanged keys in advance as long as they have a common certifier they both trust.

S/MIME works with a variety of cryptographic algorithms, such as DES, AES, and RC2 for symmetric encryption.

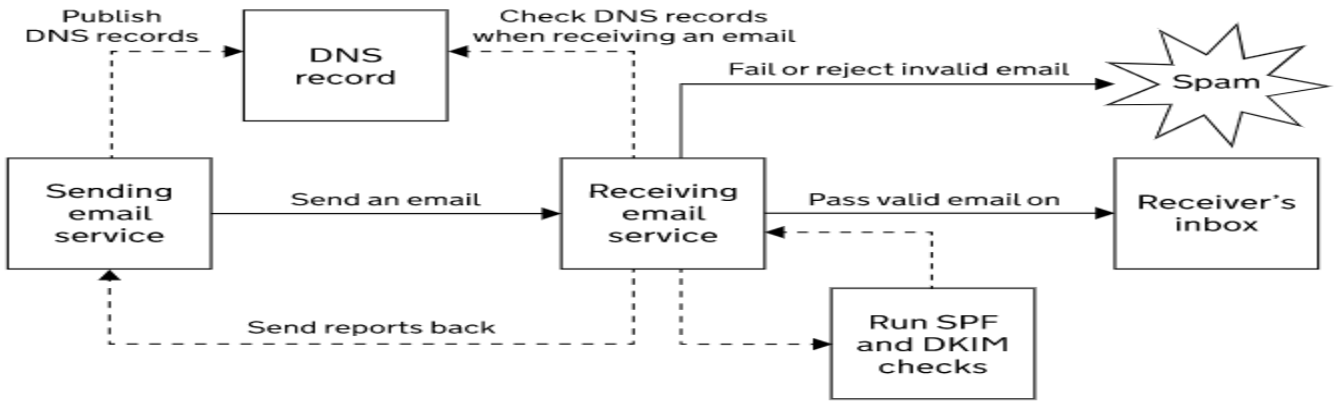
S/MIME performs security transformations very similar to those for PGP.

PGP was originally designed for plaintext messages, but S/MIME handles (secures) all sorts of attachments, such as data files (for example, spreadsheets, graphics, presentations, movies, and sound).

Because it is integrated into many commercial email packages, S/MIME is likely to dominate the secure email market.

Best Practice for companies - DMARC

- Organisations should set up DMARC which is Domain-based Message Authentication, Reporting and Conformance email standard that:
  1. confirms the sender's identity using Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM)
  2. tells the recipient's email service what to do with emails that fail the check
  3. asks recipient email services to provide reports of where email comes from



The benefit of DMARC are:

- Protecting your users, employees and reputation from cybercrime
- Reducing customer support costs relating to email fraud
- Improving trust in the emails your organisation sends
- Seeing the legitimate and fraudulent use of your domains via DMARC reports

Multi layered approach

National Cyber Security Centre
a part of GCHQ

Phishing attacks:
Defending your organisation

A multi-layered approach - such as the one summarised below - can improve your resilience against phishing whilst minimising disruption to user productivity. This approach provides multiple opportunities to detect a phishing attack and stop it before it causes major harm. The mitigations included are also useful against other types of cyber attack.

LAYER 1
Make it difficult for attackers to reach users.

- Implement anti-spoofing controls to stop your email addresses being a resource for attackers.
- Consider what information is available to attackers on your website and social media and help your users do the same.
- Filter or block incoming phishing emails.

LAYER 2
Help users identify and report suspected phishing emails.

- Relevant training can help users spot phishing emails, but no amount of training can help them spot every email.
- Help users to recognise fraudulent requests by reviewing processes that could be mimicked and exploited.
- Create an environment that lets users seek help through a clear reporting method, useful feedback and a no-blame culture.

LAYER 3
Protect your organisation from the effects of undetected phishing emails.

- Protect your accounts: make authentication more resistant to phishing (such as setting up 2FA) and ensure authorisation only gives privileges to people who need them.
- Protect your users from malicious websites by using a proxy server and an up-to-date browser.
- Protect your devices from malware.

LAYER 4
Respond quickly to incidents.

- Define and rehearse an incident response plan for different types of incidents, including legal and regulatory responsibilities.
- Detect incidents quickly by encouraging users to report any suspicious activity.

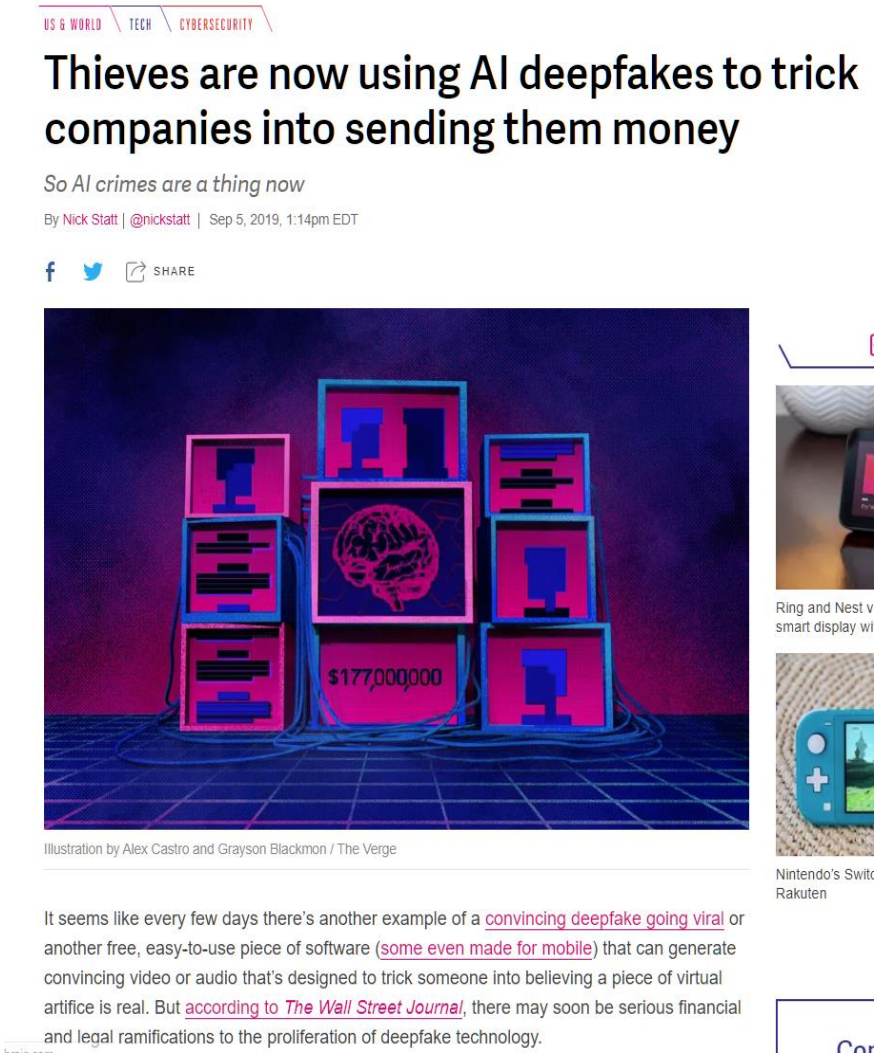
CPNI
Centre for the Protection of National Infrastructure

Deep Fake Audio Calls

In March 2019, the CEO of a large energy firm sanctioned the urgent transfer of €220,000 to what he believed to be the account of a new Eastern European supplier after a call he believed to be with the CEO of his parent company.

Within hours, the money had passed through a network of accounts in Latin America to suspected criminals who had used artificial intelligence (AI) to convincingly mimic the voice of the CEO.

With one AI-enabled conversation, criminals had bypassed layers of cybersecurity controls. Their success illustrates how certain use of powerful developing technologies such as AI will change the landscape of cybercrime for both attackers and defenders



US & WORLD \ TECH \ CYBERSECURITY

Thieves are now using AI deepfakes to trick companies into sending them money

So AI crimes are a thing now

By Nick Statt | @nickstatt | Sep 5, 2019, 1:14pm EDT

SHARE

Illustration by Alex Castro and Grayson Blackmon / The Verge

It seems like every few days there's another example of a convincing deepfake going viral or another free, easy-to-use piece of software (some even made for mobile) that can generate convincing video or audio that's designed to trick someone into believing a piece of virtual artifice is real. But according to *The Wall Street Journal*, there may soon be serious financial and legal ramifications to the proliferation of deepfake technology.

Ring and Nest v
smart display wi

Nintendo's Switc
Rakuten

Deep Fake Videos

- https://www.youtube.com/watch?v=yaq4sWFvnAY&feature=emb_logo