

## No Phishing Allowed

Charles Frank (NKU)  
Laurie Werner (Miami U Hamilton)



---

---

---

---

---

---

---

---

## Introduction to Phishing

Chuck Frank

---

---

---

---

---

---

---

---

## Phishing

- Examples (Recent Phishing Scams)
  - <http://www.millersmiles.co.uk/>
- Scam sorted by company name
  - Archive | Sorted by company name
  - <http://www.millersmiles.co.uk/>
  - Fifth Third Bank
    - [http://www.millersmiles.co.uk/search/Fifth\\_Third\\_Bank](http://www.millersmiles.co.uk/search/Fifth_Third_Bank)

---

---

---

---

---

---

---

---

## In spring, a phisher's fancy turns to taxes

- ComsumerReports.org, March 10, 2008
- "This and other scams that use refunds from the IRS as bait are more prevalent than ever."
- "There has been a 3,000 percent year-over-year increase in phishing attack and malicious Web sites targeting the IRS"

---

---

---

---

---

---

---

---

• **From:** IRS [refund@irs.gov]  
 • **Sent:** Friday, July 13, 2007 8:44 PM  
 • **Subject:** Internal Revenue Service - Tax Refund  
 • **Importance:** High

Good News,

After the last annual calculation of your fiscal activity we have determined that you are eligible to receive a tax refund of \$93.82. Please submit the tax refund request and allow us 2-4 days in order to process it.

A refund can be delayed for a variety of reason. For example (invalid records or applying after the deadline). The good news is that IRS will make this refund directly to your visa and/or mastercard linked to your checking/savings account instead a check or a direct deposit.

To access the form for your tax refund, please continue to our secure form "[Tax Refund V.M](#)".

Important: Do not use credit and/or american express or discover cards. Only cards that are linked to your checking/savings account are accepted.

Regards,

Stephen Bronner  
Internal Revenue Service - Tax Refund Specialist

---

---

---

---

---

---

---

---

## Pharming

- **Pharming** (pronounced farming) is a hacker's attack aiming to redirect a website's traffic to another, bogus website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software.

---

---

---

---

---

---

---

---

### Spear Phishing

- Attackers create email messages that are designed to look like they came from the recipient's company or organization, such as an information-technology or a human-resources department.

---

---

---

---

---

---

---

---

From: "WEBMAIL SUPPORT" <tullyseamus@XYZ-Net.net>  
 Reply-To: <web-support@UVW-Com.com>  
 To: [undisclosed]  
 Subject: Dear uwaterloo.ca Webmail Subscriber  
 Date: Sat, 29 Mar 2008 12:58:59 +0000 Dear uwaterloo.ca Webmail Subscriber,  
 To complete your uwaterloo.ca Webmail account, you must reply to this email immediately and enter your password here (\*\*\*\*\*)  
 Failure to do this will immediately render your email address deactivated from our database.  
 You can also confirm your email address by logging into your uwaterloo.ca Webmail account at <https://uwaterloo.ca>  
 Thank you for using uwaterloo.ca!  
 THE uwaterloo.ca TEAM  
 uwaterloo.ca WEBMAIL SUPPORT  
 Confirm Your E-mail Address  
 support@uwaterloo.ca

---

---

---

---

---

---

---

---

### Using Press Releases

- Forrester analyst, Paul Stamp
- The new COO received a email purportedly from the firm that does the enterprise's travel bookings. He was requested to click on the link and make sure his details were accurate.

---

---

---

---

---

---

---

---

### Using Press Releases

- He was then requested to download some software that would link his Outlook email to the travel agency's booking systems. The COO did this. Unbeknownst to the COO he was actually downloading trojan horse malware which then rapidly spread through his new enterprise.

---

---

---

---

---

---

---

---

### Whaling: Spear Phishing of the rich and powerful

- Thousands of high-ranking executives across the country have been receiving e-mail messages this week that appear to be official subpoenas from the United States District Court in San Diego. Each message includes the executive's name, company and phone number, and commands the recipient to appear before a grand jury in a civil case.

---

---

---

---

---

---

---

---

### Whaling

- A link embedded in the message purports to offer a copy of the entire subpoena. But a recipient who tries to view the document unwittingly downloads and installs software that secretly records keystrokes and sends the data to a remote computer over the Internet. This lets the criminals capture passwords and other personal or corporate information.

---

---

---

---

---

---

---

---

## Whaling




---

---

---

---

---

---

---

---

---

---

---

---

## Vishing

- VoIP allow caller ID spoofing
- Uses war dialing
- When a victim answers, an automated voice system alerts the consumer of fraudulent activity on the credit card or unusual activity in their bank account and asks them to call a number.

---

---

---

---

---

---

---

---

---

---

---

---

## Vishing

- Sometimes Vishing uses email directing the consumer to call a number.
- When they call this number, an automated system asks them to key in their credit card number or bank account number.

---

---

---

---

---

---

---

---

---

---

---

---

**From:** hallmark.com [E-Cards@hallmark.com]  
**Sent:** Tuesday, August 28, 2007 4:20 PM  
**To:** Charles Frank  
**Subject:** You've received A Hallmark E-Card!

**Follow Up Flag:** Follow up  
**Flag Status:** Completed

**You have recieved A Hallmark E-Card.**

Hello!

You have recieved a Hallmark E-Card.

To see it, click [here](#).

There's something special about that E-Card feeling. We invite you to make a friend's day and [send one](#).

Hope to see you soon,  
Your friends at Hallmark

Your privacy is our priority. Click the "Privacy and Security" link at the bottom of this E-mail to view our policy.

[Hallmark.com](#) | [Privacy & Security](#) | [Customer Service](#) | [Store Locator](#)

---

---

---

---

---

---

---

---

---

---

---

---

Dharmija, Tyger and Hearst,  
 "Why Phishing Works"

- Good phishing web sites fooled 90% of participants.
- Twenty-three percent of the college-educated participants did not look at browser-based cues such as the address bar, status bar and the security indicators, leading to incorrect choices 40% of the time.

---

---

---

---

---

---

---

---

---

---

---

---

Dharmija, Tyger and Hearst,  
 "Why Phishing Works"

- Found that some visually deceptive attacks can fool even the most sophisticated users.
- Neither education, age, sex, previous experience, nor hours of computer use showed a statistically significant correlation with vulnerability to phishing.

---

---

---

---

---

---

---

---

---

---

---

---

Ryan West,  
"The Psychology of Security"

- Risk is difficult for people to evaluate
  - Users are likely to make quick decisions without considering the risks and consequences.
  - The concrete reward offered by a phishing email can be more compelling than the abstract reward of security
- Non-acceptance of security tools is a major problem

---

---

---

---

---

---

---

---

Michael Gibbons, 38, of Houston, Texas, last December responded to an e-mail he thought was from eBay, urging him to update his account information for "security reasons." After clicking on a link in the e-mail, Gibbons, who buys and sells books and other kinds of merchandise online, was taken to a bogus eBay site.

In a lapse of judgment that he would later describe as the "beginning of a long, major life lesson," Gibbons entered his eBay ID and password, his address, checking and credit card account numbers and expiration dates, bank routing and Social Security numbers, his birthday, his mother's maiden name and his bank card PIN.

Within hours, scammers siphoned \$1,500 from his debit card account and changed his e-mail and eBay account passwords. They even locked Gibbons out of his bank account by securing it with a password of their own.

---

---

---

---

---

---

---

---

Delores Hanes, 77, is one of those people. The Vancouver, Wash., resident fell victim to a phishing scam targeting customers of PayPal, eBay's online payment subsidiary.

"It had the PayPal pictures all over," Hanes said. "On the surface at least it looked like everything else I'd seen from them."

Hanes and her husband Bob, 80, first realized something was amiss when a woman from Western Union called to confirm that they authorized a \$200 electronic payment to someone in Germany. Soon, checking charges appeared for amounts ranging from \$50 to \$150, including a request to open a new Internet service account with America Online, Hanes said.

"For days I couldn't eat, couldn't sleep at night, I was so upset," Hanes said.

Even after countless hours on the phone with her bank, the charges kept coming. Mrs. Hanes said the experience so rattled her that she and her husband have sworn off e-commerce for good.

---

---

---

---

---

---

---

---

### Phishing Consequences

- Online scams are weakening e-mail as a trustworthy method of communication between companies and their customers
- The scammers are really beginning to poison the well of e-commerce to the point where many people can no longer tell the difference between what's fake and what's legitimate

---

---

---

---

---

---

---

---

### Status of Phishing Today

Laurie Werner




---

---

---

---

---

---

---

---

### Status of phishing today

**Antiphishing Working Group (APWG) tracks:**

- Unique phishing email campaigns
- Unique phishing websites determined by unique base URLs of the phishing sites
- Crimeware instances (determined by MD5 hash of the crimeware sample)
- Unique sites that are distributing crimeware




---

---

---

---

---

---

---

---

### Status of phishing today

- **Antiphishing Working Group (APWG) first quarter 2008 reports that:**
  - **Crimeware & Crimeware-Spreading URL Stats Break All Records**
  - **Crimeware-spreading URLs infecting PCs with password-stealing code rose 93 percent to 6,500 sites**
    - This is nearly double the previous high of November, 2007
    - This is an increase of 337 percent from the number detected end of Q1, 2007




---

---

---

---

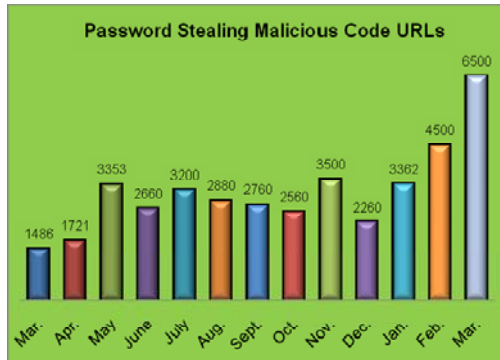
---

---

---

---

### March 2007-March 2008




---

---

---

---

---

---

---

---

### Status of Phishing Today

- **The number of unique keyloggers and crimeware-oriented malicious applications detected rose to 430 in March, 2008**
  - **an all-time record some 18 percent greater than the previous record month of January, 2008, when 364 unique malicious applications were detected.**




---

---

---

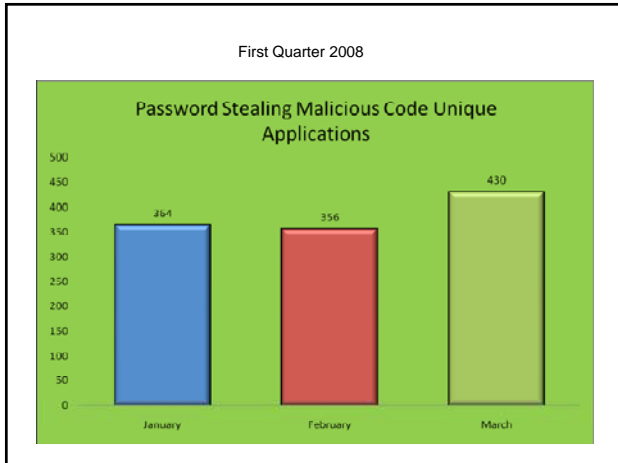
---

---

---

---

---




---

---

---

---

---

---

---

---

### An Example of A Crimeware Phish

- Social networks are services used by millions of users. Such popularity has not gone unnoticed by cyber-crooks who have started to distribute their creations through these pages more frequently.
- Twitter, one of the most famous microblogging services, was one of the latest networks to be attacked. PandaLabs, Panda Security's laboratory for detecting and analyzing malware, detected the **Dadobra.AQI Trojan**, distributed through Twitter using social engineering. In this case, the messages tempted users into clicking on a link to view supposed erotic photos of the Brazilian singer Kelly Key. On clicking the link users were redirected to a page which required they download a version of Adobe Flash to view the images. On doing so, a copy of the Trojan was downloaded onto their computer.

---

---

---

---

---

---

---

---

### Why the rise in crimeware-spreading URLs

- Profitability potential: big phish, big results
- Ease of setup – kits available on-line (Panda reported 15000 hits on a website offering the kits)
- Perpetrators out of the country are out of reach of the FBI
  - Recent whaling of top executives reported in the NY times last Spring targeted executives, traced to China
- APWG reports that it takes as much as 30 days to take down a phishing website once it is found

---

---

---

---

---

---

---

---

### Status of Phishing Today

- The most targeted industry sector continues to be Financial Services
- US continues to be the top country hosting phishing sites
- US is the top country hosting Phishing-based Trojans and Trojan downloaders
- The number of Hijacked brands remains in the 120-160 per month range

---

---

---

---

---

---

---

---

### Status of Phishing today

- Phishing increasing in incidence numbers and in sophistication



---

---

---

---

---

---

---

---

### Anti-Phishing Products

Chuck Frank

---

---

---

---

---

---

---

---

### Consumer Report Antiphishing Tools 9/2008

- McAfee SiteAdvisor
  - Free add-on (Quick Pick)
  - Comes bundled with McAfee Internet Security Suite
- Microsoft Internet Explorer 7
  - Browser (Quick Pick)
  - Need to active “Automatic Phishing Filter” during installation

---

---

---

---

---

---

---

---

### Consumer Report Antiphishing Tools 9/2008

- Netcraft Toolbar
  - Free add-on (Quick Pick)
- Symantec Norton Internet Security 2008
  - Suite Component
- Trend Micro Internet Security 2008
  - Suite Component
- Firefox 3
  - Was too new to rate

---

---

---

---

---

---

---

---

### Netcraft Toolbar

- Firefox Add-on
- Blocks phishing sites
- <http://toolbar.netcraft.com/>

---

---

---

---

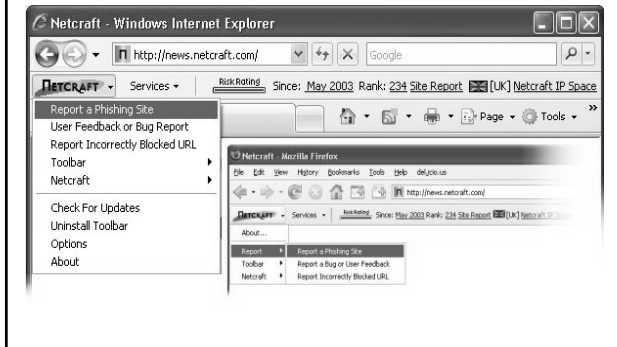
---

---

---

---

## Netcraft Toolbar




---

---

---

---

---

---

---

---

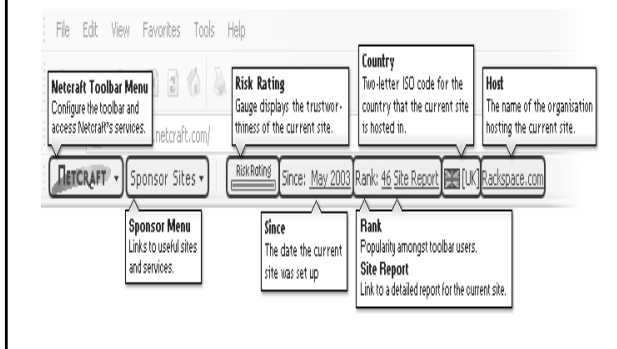
---

---

---

---

## Netcraft Toolbar




---

---

---

---

---

---

---

---

---

---

---

---

### Frei, Dübendorfer, Ollmann, May, "Understanding the Web browser threat"

- Attacks against Web browsers depend upon malicious content being rendered by the appropriate built-in interpreter (e.g., HTML, JavaScript, CSS, etc.) or vulnerable plug-in technology (e.g., Flash, QuickTime, Java, etc.)
- Profit motivated cyber-criminals have rapidly adopted Web browser exploitation as a key vector for malware installation.

---

---

---

---

---

---

---

---

---

---

---

---

Frei, Dübendorfer, Ollmann, May,  
"Understanding the Web browser threat"

- The data used to measure the worldwide vulnerable Web browser population within each browser type was provided by Google.
- The tip of the Web browser insecurity iceberg was measured to be 637 million (or 45.2%) Internet users at risk worldwide due to not running the latest most secure browser version. Meanwhile, hidden below the surface, the iceberg extends further encompassing users that rely on outdated vulnerable browser plug-ins.

---

---

---

---

---

---

---

---

## Phishing Education

Laurie Werner



---

---

---

---

---

---

---

---

## Education (Laurie)

- Higher Education
  - Computing majors
  - General education
- K-12
- On-the-Job

---

---

---

---

---

---

---

---

## Current Trends in InfoSec Higher Education Emphasize Phishing

- Two main threads in areas of concentration
  - Anti-phishing
    - Authentication, DNS signing, email signing, cryptography
  - Virtual OS Sandbox
- Two principles Necessary For Anti-Phishing Success
  - Understand how current security fails
  - Know architecture fundamentals
    - Include history of security
    - Provide the larger picture of how physical and personal security come together

---

---

---

---

---

---

---

---

## According to Spafford (9/8/08)

- Education provides a grounding and a basis for using current security tools and the knowledge to extend and improve the security tools
- Training provides skills with current tools
- Both education and training are needed
- “You could almost give a graduate degree in phishing.”

---

---

---

---

---

---

---

---

## Phishing in Computing Literacy

- Students are interested in protecting themselves from threats
- There are teaching tools and websites
  - Phishing IQ test – HS, college and all email users
  - Anti-phishing Phil – younger users by nature of the game aspect

---

---

---

---

---

---

---

---

### Phishing IQ test

- <http://www.sonicwall.com/phishing/>

---

---

---

---

---

---

---

---

### Phishing IQ Test Sample Question: Is this phishing or legitimate?




---

---

---

---

---

---

---

---

### Sample Explanation showing what to look for in the email




---

---

---

---

---

---

---

---



### On-the-Job

- Students graduating with CS or IT degrees know about Information Assurance, and such important topics as phishing, but may have no practical experience in any aspect of security, and thus must learn on the job.

---

---

---

---

---

---

---

---

### Frank & Werner, “Getting A Hook On Phishing”

Chuck Frank

---

---

---

---

---

---

---

---

### Frank & Werner, “Getting A Hook On Phishing”

- Labs to teach students about phishing
  - Some can be used in computer literacy courses
  - Some are for computer science/information technology majors
  - Could be used to train employees and IT staff in phishing

---

---

---

---

---

---

---

---

### Phishing Labs

- Lab #1 Phishing IQ Test
- Lab #2 Analysis of Phishing
  - Analyzing phishing emails and Web site at <http://www.millersmiles.co.uk/>
- Lab #3 Spoofing Email
  - How to easily spoof the sender of an email
- Lab #4 Phishing Web site
  - Create a fake login page that looks authentic

---

---

---

---

---

---

---

---

### Phishing Labs

- Lab #5 Phishing Email
  - Create a phishing email directing to phishing Web site
- Lab #6 Phroogle
  - Explore potential phishing manipulation of a shop-bot like Google shopping (due to Jakobsson & Myers)

---

---

---

---

---

---

---

---

### Frank & Werner Phishing Labs

- Analysis of Phishing Lab (2007) web site, <http://www.nku.edu/~frank/phishing/Analysis.htm>.
- Phishing Email Lab (2007) web site, <http://www.nku.edu/~frank/phishing/Email.htm>.
- Phishing IQ Test Lab (2007) web site, <http://www.nku.edu/~frank/phishing/PhishingIQTest.htm>.
- Phishing Web Site Lab (2007) web site, <http://www.nku.edu/~frank/phishing/WebSite.htm>.
- Phroogle Lab (2007) web site, <http://www.nku.edu/~frank/phishing/Phroogle.htm>
- Spoofed Email Lab (2007) web site, <http://www.nku.edu/~frank/phishing/SpoofedEmail.htm>.

---

---

---

---

---

---

---

---

## Recommendations

Chuck Frank

---

---

---

---

---

---

---

---

## Attacking Phishing

- Education
- Policies
- Technology
- Laws
- Unfortunately, nothing works really solves the problem.

---

---

---

---

---

---

---

---

## Good Practices

1. Don't click on email links
2. Don't believe in strident calls to action
3. Don't click on suspicious links
4. Only enter information on the expected site
5. Check for the lock icon, and only enter confidential information using a valid SSL session

---

---

---

---

---

---

---

---

## Need Better Practices by Financial Institutions

- Some financial institutions emails to user and Web pages violate these best practices
- Example, clickable links in emails that are part of a marketing campaign
- Practices are improving
- Good practice: Vanguard and Discover always ask user to type in URL on browser

---

---

---

---

---

---

---

---

## Digitally Signed Emails

- Use S/MIME to verify the sender is legitimate
- Supported by Microsoft Outlook
- Deployment problem
- Usability problem

---

---

---

---

---

---

---

---

## Bruce Schneier

- Financial institutions have no incentive to reduce the costs of identity theft because they don't bear it.
- Push the responsibility on financial institutions.
- Security works best when the entity that is the best position to mitigate the risk is responsible for that risk.

---

---

---

---

---

---

---

---

### Anti-Phishing Act of 2005

- Senator Leahy’s bill
- Criminalize the act of creating a phishing web site and the sending of phishing emails regardless of whether there was a victim
- Referred to the Judiciary Committee

---

---

---

---

---

---

---

---

### Bibliography

- Anti-Phishing Phil Web site, [http://cups.cs.cmu.edu/antiphishing\\_phil/](http://cups.cs.cmu.edu/antiphishing_phil/)
- AuthenticationWorld Blog, “Targeted spear phishing example”, [http://www.authenticationworld.com/blog/2006/12/targeted\\_spear\\_phishing\\_exempl.html](http://www.authenticationworld.com/blog/2006/12/targeted_spear_phishing_exempl.html)
- ConsumerReports.org, “Ratings: Antiphishing tools”, [http://www.consumerreports.org/cro/electronics-computers/computers/software/security-software/antiphishing-tools\\_ratings/ratings/security-software-antiphishing-tools\\_ratings.htm?resultPageIndex=1&resultIndex=1&searchTerm=antiphishing%20tools](http://www.consumerreports.org/cro/electronics-computers/computers/software/security-software/antiphishing-tools_ratings/ratings/security-software-antiphishing-tools_ratings.htm?resultPageIndex=1&resultIndex=1&searchTerm=antiphishing%20tools)
- ConsumerReports.org, “In spring, a phisher’s fancy turns to taxes”, <http://blogs.consumerreports.org/electronics/2008/03/in-spring-a-phi.html?resultPageIndex=1&resultIndex=2&searchTerm=IRS%20phishing>

---

---

---

---

---

---

---

---

### Bibliography

- Dhamija, Rachna, Tygar, J. D., and Hearst, Marti, “Why phishing works”, Proceedings of the SIGCHI conference on Human Factors in computing systems, April 22-27, 2006, Montréal, Québec, Canada, pp. 581- 590.
- Frank, C and L Werner (2007). Getting A Hook On Phishing. *Information Systems Education Journal*, 5 (36), <http://isedj.org/5/36/index.html>.
- Stefan Frei, Thomas Dübendorfer , Gunter Ollmann , Martin May, "Understanding the Web browser threat: Examination of vulnerable online Web browser populations and the ‘insecurity iceberg’", <http://www.techzoom.net/publications/insecurity-iceberg/>
- Griffin, S. and Rackely, C. Vishing, InfoSecCD 2008 Proceedings
- Jakobsson, Markus and Myers, Stephen, (2007), Phishing and Countermeasures, Wiley-Interscience, New Jersey.

---

---

---

---

---

---

---

---

## Bibliography

- James, Lance, (2005), Phishing Exposed, Syngress Press, Massachusetts
- Larcom, G. and Elbirt, A.J., "Gone Phishing", IEEE Technology and Society Magazine, Fall 2006.
- Markoff, John, "Large Prey Are Targets of Phishing", New York Times, April 16, 2008, [http://www.nytimes.com/2008/04/16/technology/16whale.html?\\_r=1&oref=slogin](http://www.nytimes.com/2008/04/16/technology/16whale.html?_r=1&oref=slogin)
- Millersmile.uk.co Web site (the web's dedicated anti-phishing service), <http://www.millersmiles.co.uk/>
- Phishing Schemes Scar Victims, <http://www.washingtonpost.com/ac2/wp-dyn/A59349-2004Nov18?language=printer>

---



---



---



---



---



---



---

## Bibliography

- Purdue University resources for elementary and HS teachers, <http://www.cerias.purdue.edu/education/k-12/>
- Schneier, Bruce, "A Real Remedy for Phishers", <http://www.schneier.com/essay-090.html>
- SonicWall Phishing IQ Test (2007) web site, <http://www.sonicwall.com/phishing/>
- University of Waterloo, Canada, Spear Phishing Example, <http://ist.uwaterloo.ca/security/vulnerable/20080403/20080329.html>
- Vishing, <http://en.wikipedia.org/wiki/Vishing>.
- West, Ryan, "The Psychology of Security", Communications of the ACM, Volume 51 Issue 4 (April 2008), pp. 34-40

---



---



---



---



---



---



---