

Phishing Attacks

Mendel Rosenblum

Phishing

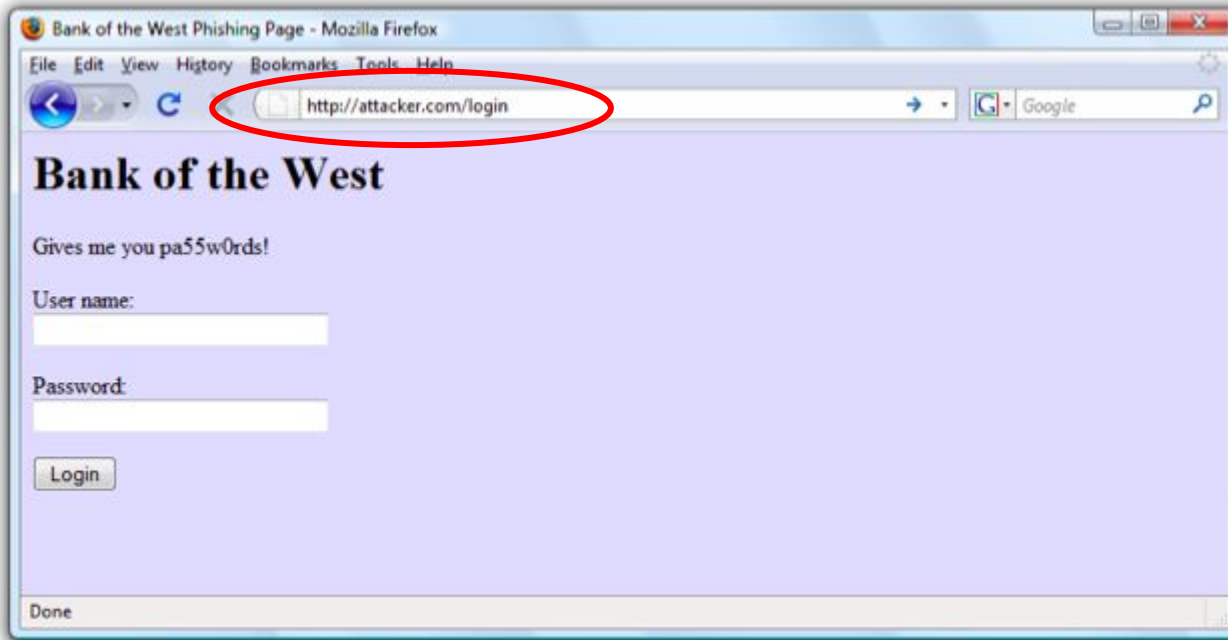
- Basic idea:
 - Get unsuspecting users to visit an evil Web site
 - Convince them that the evil Web site is actually a legitimate site (such as a bank or PayPal)
 - Trick the user into disclosing personal information (password, credit card number, etc.)
 - Use the personal information for evil purposes such as identity theft.
- How to attract users?

Spoofing legitimate sites

How to spoof the legitimate site?

- Copy HTML
- Include images from legitimate Web site
- Many links refer back to the legitimate Web site
- After collecting login info, log user into legitimate site, redirect to legitimate site
- User has no idea that password has been stolen

URL could be obviously Illegitimate



Or very subtly different: Look-alike characters



International Character Sets

- What does this URL refer to:

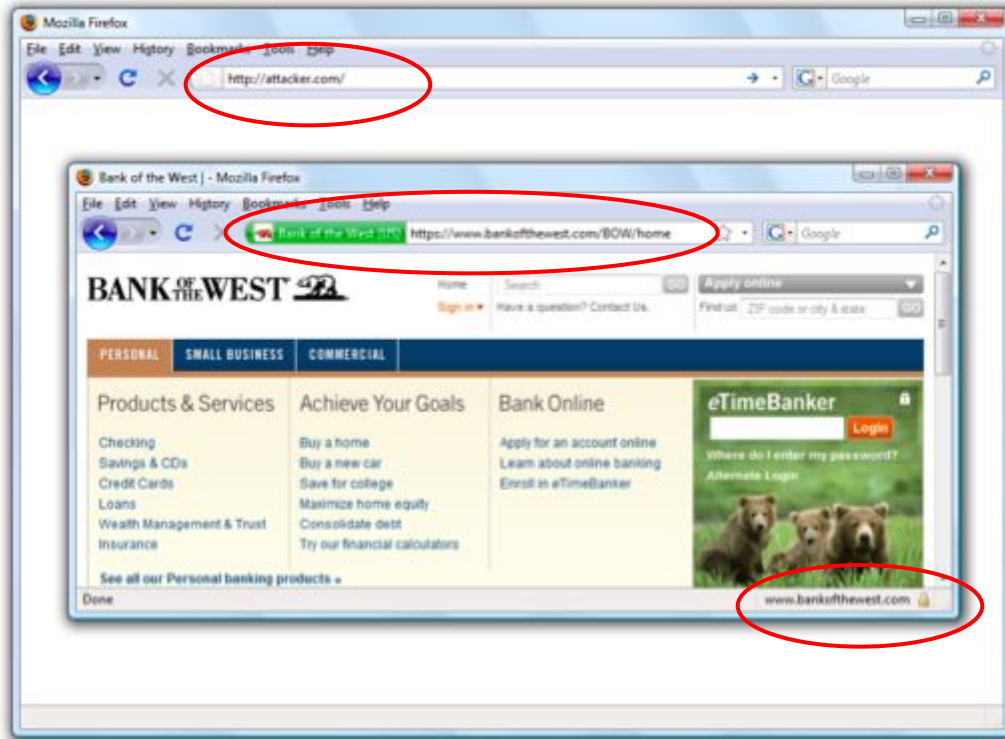
www.bank.com/accounts/login.php?q=me.badguy.cn

Chinese characters that look like "/", "?", and "="

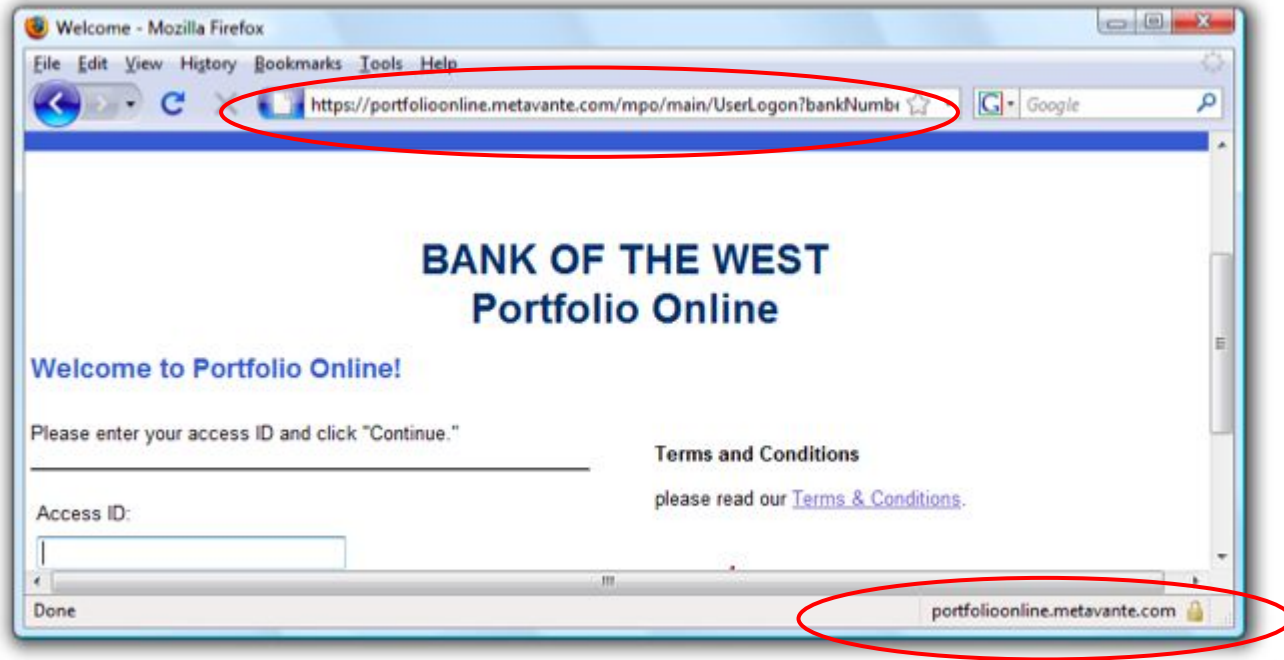


- This is a host name only!

Picture in picture



Legitimate Partners Can Look Fishy



Counter-measure: visual indicators

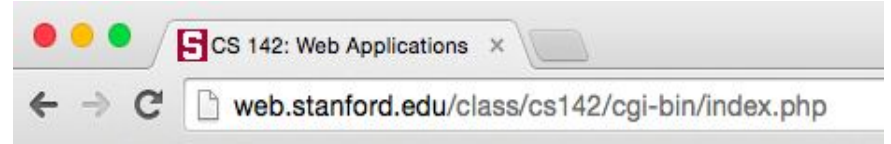
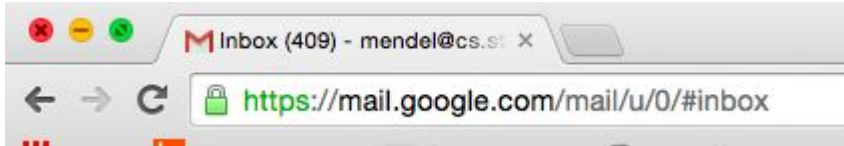
- Help users identify legitimate sites:
- Lock symbols to indicate HTTPS
 - Color change to indicate HTTPS

Problems:

- Lock symbols not always obvious

HTTPS Indicators

Chrome



Safari



Firefox



Problem: too easy to obtain certificates

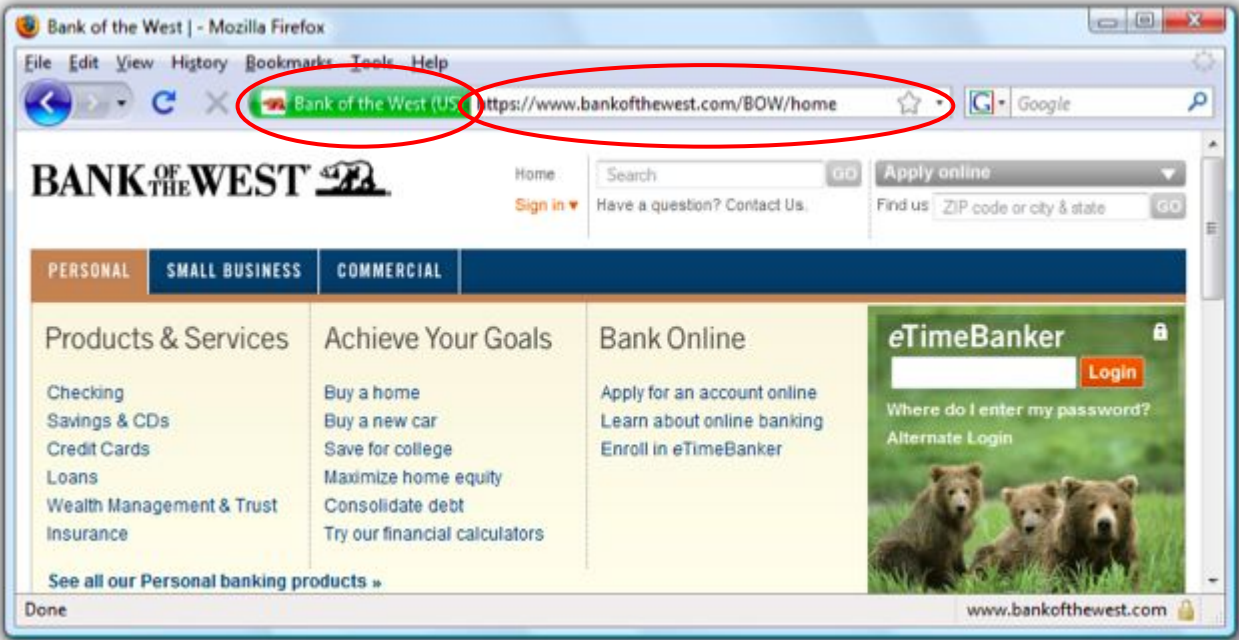
Problem: too easy to obtain certificates that look like legitimate sites

- Example: bankofamerica-secure.com
- Pressure on certificate authorities to issue certificates quickly
- E.g. "domain validation only" certificates: certificate authority only verifies that applicant has right to a particular Internet domain name; no verification of legal status of organization.

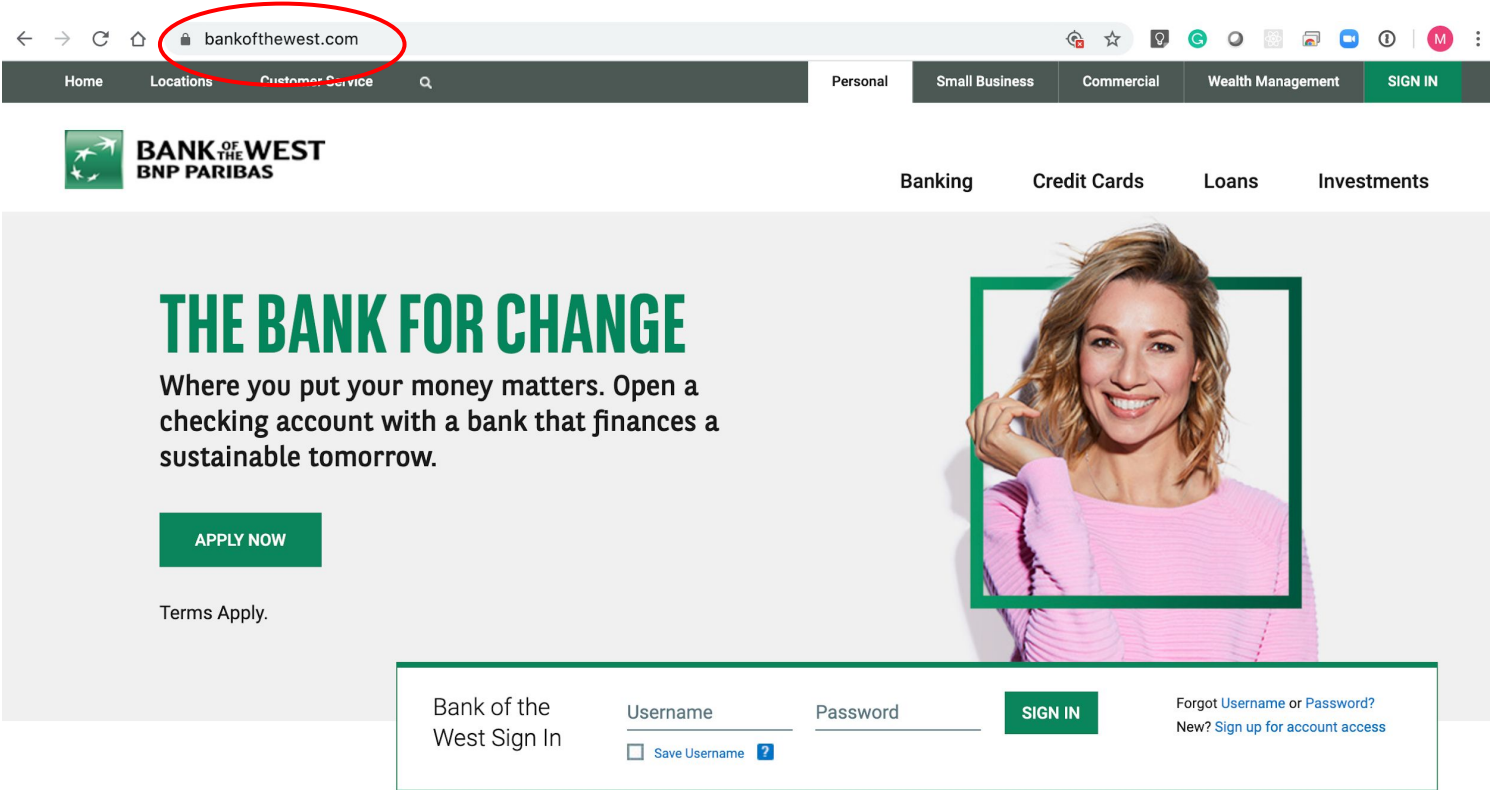
Counter-measure: extended validation certificates

- Goal: prevent attackers from obtaining certificates that look like legitimate sites
- Certificate authority must thoroughly vet the organization obtaining the certificate; prevent look-alike names.
- Certificate authority must undergo audits to ensure it is doing the vets carefully.
- Browser provides special indicator for extended validation sites
- Problems:
 - Small organizations don't like delays and cost of extended validation
 - Browsers are getting rid of indication of HTTPS (including extended) since everything has it.

Extended Validation Certificates a few years ago



Extended Validation Certificates today



The screenshot shows the top portion of the Bank of the West website. The browser's address bar at the top contains the URL 'bankofthewest.com', which is circled in red. Below the address bar is a dark navigation bar with links for 'Home', 'Locations', 'Customer Service', and a search icon. To the right of these links are tabs for 'Personal', 'Small Business', 'Commercial', 'Wealth Management', and a green 'SIGN IN' button. The main content area features the Bank of the West logo (BNP PARIBAS) on the left and navigation links for 'Banking', 'Credit Cards', 'Loans', and 'Investments' on the right. A large promotional banner is centered, with the headline 'THE BANK FOR CHANGE' in green. Below the headline is the text: 'Where you put your money matters. Open a checking account with a bank that finances a sustainable tomorrow.' A green 'APPLY NOW' button is positioned below this text. To the right of the text is a photograph of a smiling woman with blonde hair, wearing a pink sweater, framed by a green border. At the bottom of the page, a white sign-in box contains the text 'Bank of the West Sign In' on the left. In the center, there are input fields for 'Username' and 'Password', a green 'SIGN IN' button, and a checkbox labeled 'Save Username' with a question mark icon. On the right side of the sign-in box, there are two links: 'Forgot Username or Password?' and 'New? Sign up for account access'.

bankofthewest.com

Home Locations Customer Service

Personal Small Business Commercial Wealth Management SIGN IN

BANK OF THE WEST
BNP PARIBAS

Banking Credit Cards Loans Investments

THE BANK FOR CHANGE

Where you put your money matters. Open a checking account with a bank that finances a sustainable tomorrow.

[APPLY NOW](#)

Terms Apply.

Bank of the West Sign In

Username Password [SIGN IN](#)

Save Username ?

[Forgot Username or Password?](#)
[New? Sign up for account access](#)

Other counter-measures:

- Browsers starting to include anti-phishing measures (warn users about known phishing sites)
- Legitimate Web sites can monitor traffic; changes may indicate attacks under way:
 - Spike in download rates for official images
 - Unusual rate of password changes, funds transfers
- Legitimate sites can incorporate personal information in emails to authenticate them: phishers won't have such information.
 - **Spear phishing** - Phishing with attacker having personal information

Other issues

- Legitimate Web sites often use deceptive techniques to get users to click through ("your last chance for ..."), which reduces distinction between honest and dishonest sites.
- Education ineffective against phishing: response rates to phishing e-mails comparable to those for "legitimate" commercial e-mail.
- Warnings about shady certificates are ineffective: people just click through.

Two examples in the news

- Snapchat divulged employee information in phishing attack
 - “Last Friday, Snapchat’s payroll department was targeted by an isolated email phishing scam in which a scammer impersonated our Chief Executive Officer and asked for employee payroll information, ...
- Stanford staff member and student got an email with a Word doc they opened
 - Word doc contained a macro that encrypted the user's home directory and provided instruction how how to buy the encryption key.
 - **Ransomware**
 - Memo: Stanford won't reimburse you for paying ransoms