Phishing

Junxiao Shi, Sara Saleem

University of Arizona

Apr 23, 2012

What is Phishing

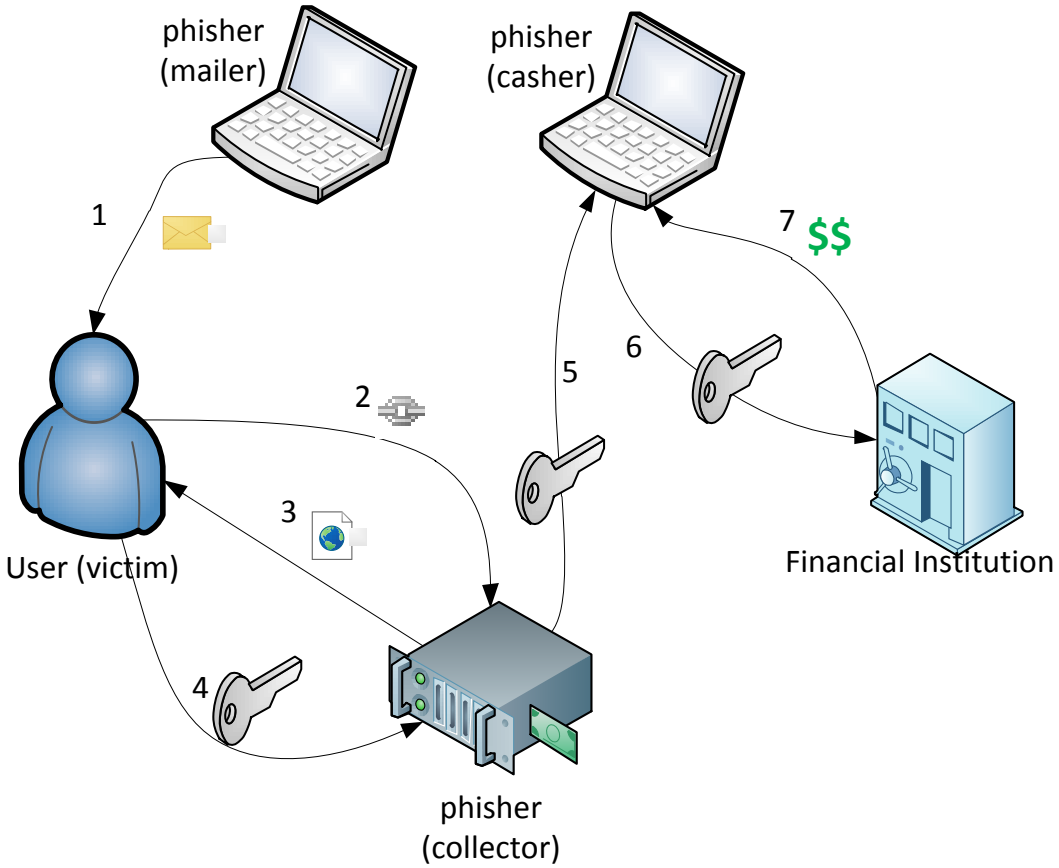
- a form of social engineering
- to fraudulently retrieve legitimate users' confidential or sensitive credentials
- by mimicking electronic communications from a trustworthy or public organization
- in an automated fashion

Phisher

Labor specialization of phishers:

- **Mailers** send out a large number of fraudulent emails (usually through bot-nets), which direct users to fraudulent websites
- **Collectors** set up fraudulent websites (usually hosted on compromised machines), which actively prompt users to provide confidential information
- **Cashers** use the confidential information to achieve a pay-out

Information Flow



Information flow in a phishing attack

Email Spoofing

- Definition: sending an email that claims to be originating from one source, when it was actually sent from another.
- DiscoverCard members are more likely to believe in an email from `support@discover.com` than from an unrelated domain.
- When you believe in an email, you may take actions according to its instructions, such as:
  - reply to the email with your credit card number
  - click on the link labelled as "view my statement", and enter your password when the website prompts for it
  - open an attached PDF form, and enter confidential information into the form

Email Spoofing

Read the report for:

- Why email spoofing is so easy?
- How to send a spoofed email with one line of command?
- What are the countermeasures?

Web Spoofing

1. Set up a forged website
2. Attract traffic to the forged website
3. Collect confidential information entered by users

Creating a forged website

1. Save the Facebook login page as an HTML file, along with images and scripts.
2. Write a PHP script that stores the submitted fields into a file or database, then redirect to the real Facebook.
3. Open the HTML file with a text editor, find the login form, and change the submission URL to that PHP script.
4. Upload these files to a PHP-enabled web server.

-or-

1. Configure a "reverse proxy" using `squid` or `Fiddler2`.
2. Write a plug-in that automatically collects information entered by users.

Attracting traffic to forged website

- Send spoofed emails with a link to the forged website.
- Register a domain that is a common typo, such as `facebok.com`.
  (Facebook registered this domain before you)
- Register the same domain name in a different TLD. For example, register `facebook.com.cn`, and translate the forged website to Chinese.
- Use pharming.

Legitimate website VS forged website

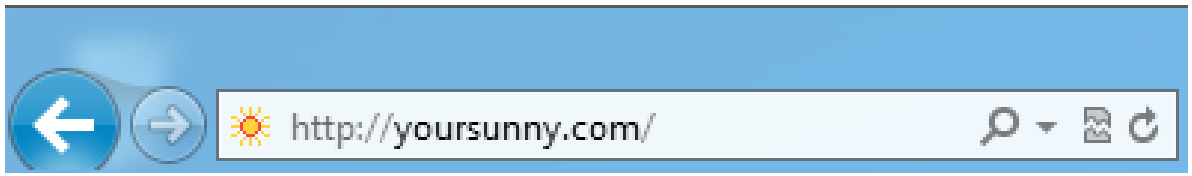
`https://www.phish-no-phish.com/`

How to tell whether a website is legitimate or forged?

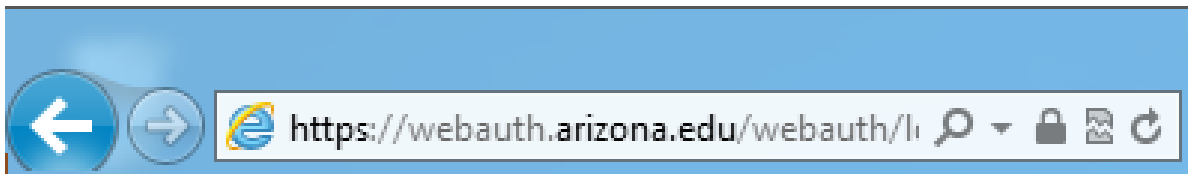
- content
- domain name
- usage of https
- certificate

Browser Security Indicator: https padlock

HTTPS, the combination of Hypertext Transfer Protocol and Transport Layer Security, provides encryption and identification through public key infrastructure. Modern web browsers display a padlock icon when visiting an https website.



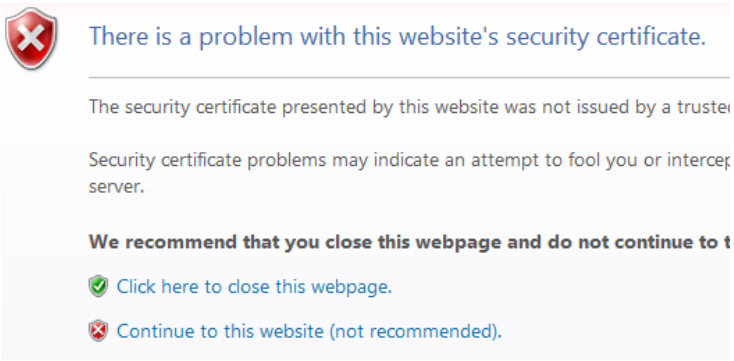
http scheme, no padlock



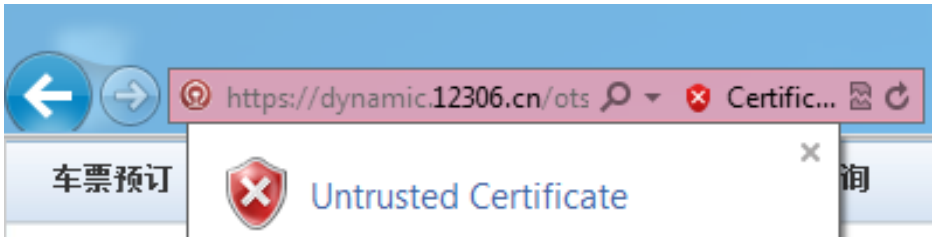
https scheme, padlock in address bar

Browser Security Indicator: https padlock

If the certificate is invalid or does not match the domain name, modern browsers will show a prominent warning.



a warning page is shown on detecting an untrusted certificate



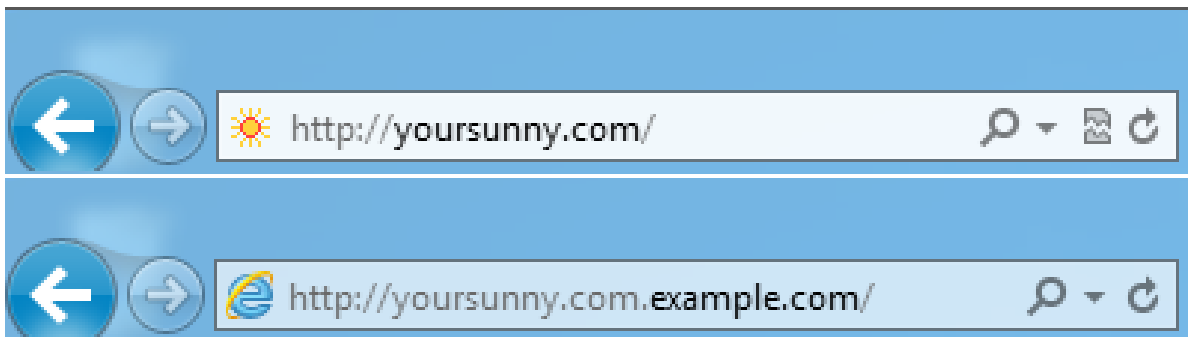
if the user chooses to continue, address bar turns red

Browser Security Indicator: EV

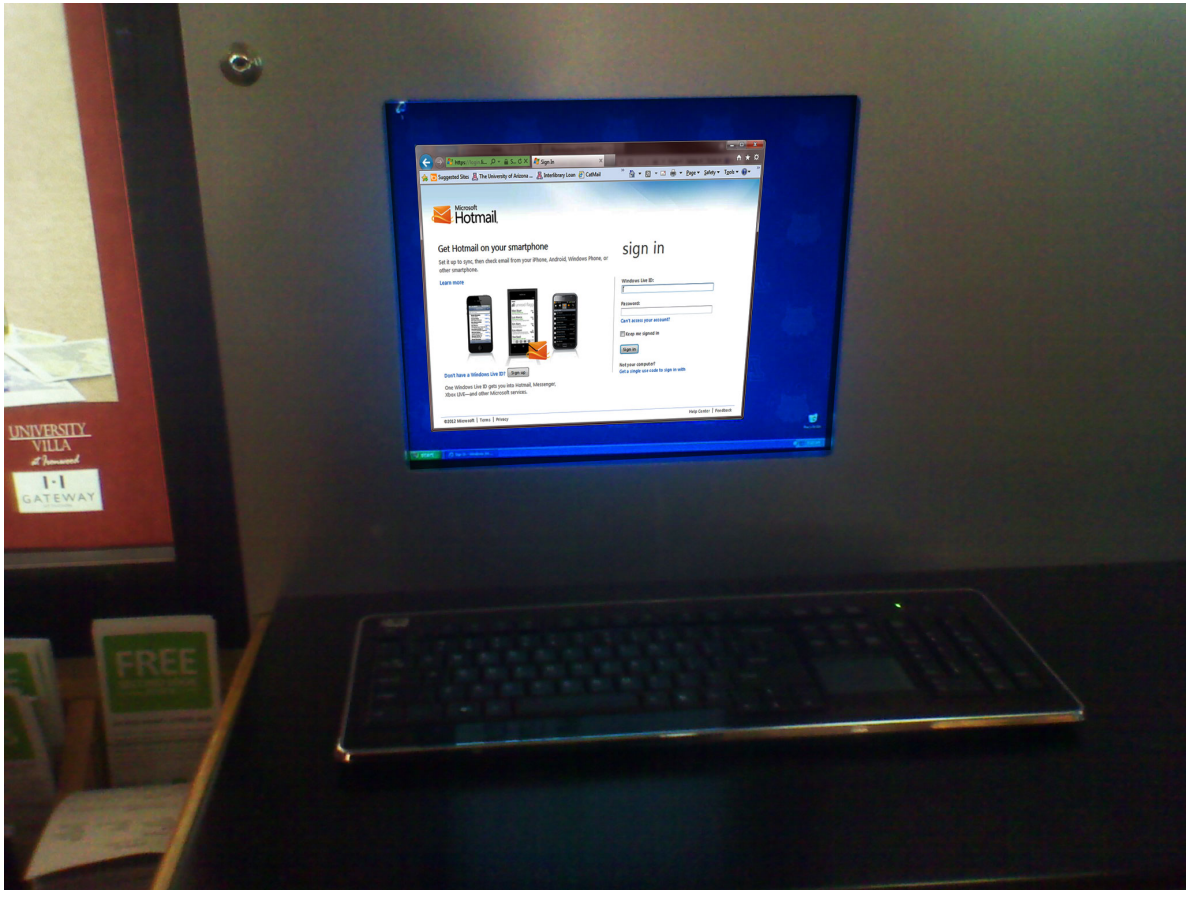
Extended Validation (EV) Certificates are only issued after extensive verification on the requesting entity: physical presence, domain control, legal documents.
Modern browsers "turn green" to indicate higher level of trust.

Browser Security Indicator: domain name highlighting

Phishers tend to use misleading addresses, such as `http://www.paypal.com.cgi-bin.webcr.example.com/`, to deceive users. With domain name highlighting, users can easily interpret the address and identify the current website at a glance.



Simulated Browser Attack



public terminal in Student Union Memorial Center Food Court

- https? Yes.
- Padlock? Yes.
- Green address bar? Yes.
- Trusted?

Simulated Browser Attack

- but, is this a real Internet Explorer?
- Probably not.
  1. A web page or Flash movie simulates the user interface and behavior of Internet Explorer.
  2. Address bar, padlock icon, status bar are all fake.
  3. Open in a chromeless window or enter full screen mode.
- Everything you enter goes to the phisher; web pages you see may be modified by the phisher.
- That's why you shouldn't use online banking on public computers.

Pharming

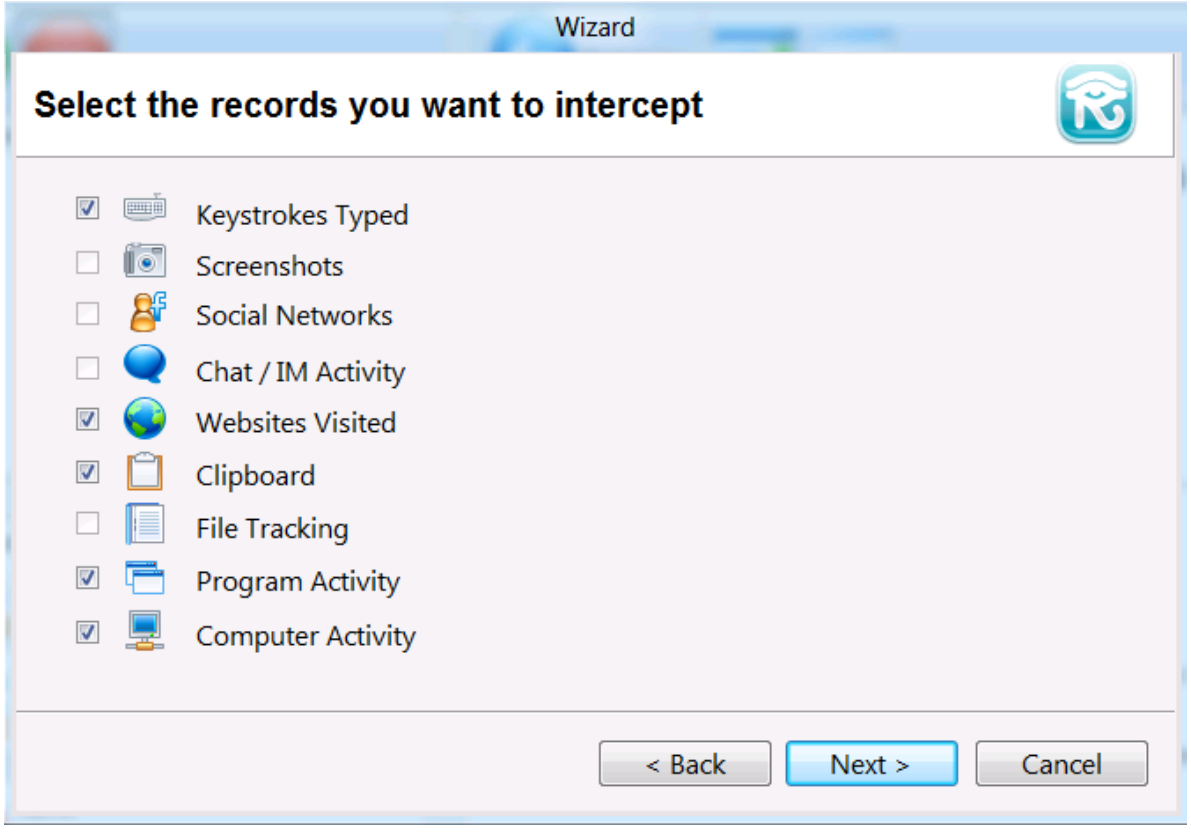
Pharming: a type of attack intended to redirect traffic to a fake Internet host.
Read the report for:

- DNS cache poisoning, and its countermeasures
- Domain hijacking, the pharming method with global effects
- Long term, unnoticeable pharming in local computer or a home network

Malware

- Malware: a piece of software developed either for the purpose of harming a computing device or for deriving benefits from it to the detriment of its user.
- In phishing, malware can be used to collect confidential information directly, and send them to phishers.
  - Keystrokes, screenshots, clipboard contents, and program activities can be collected
  - Malware can display a fake user interface to actively collect information.
  - Collected information can be automatically sent to phishers by email, ftp server, or IRC channel.

Keylogger

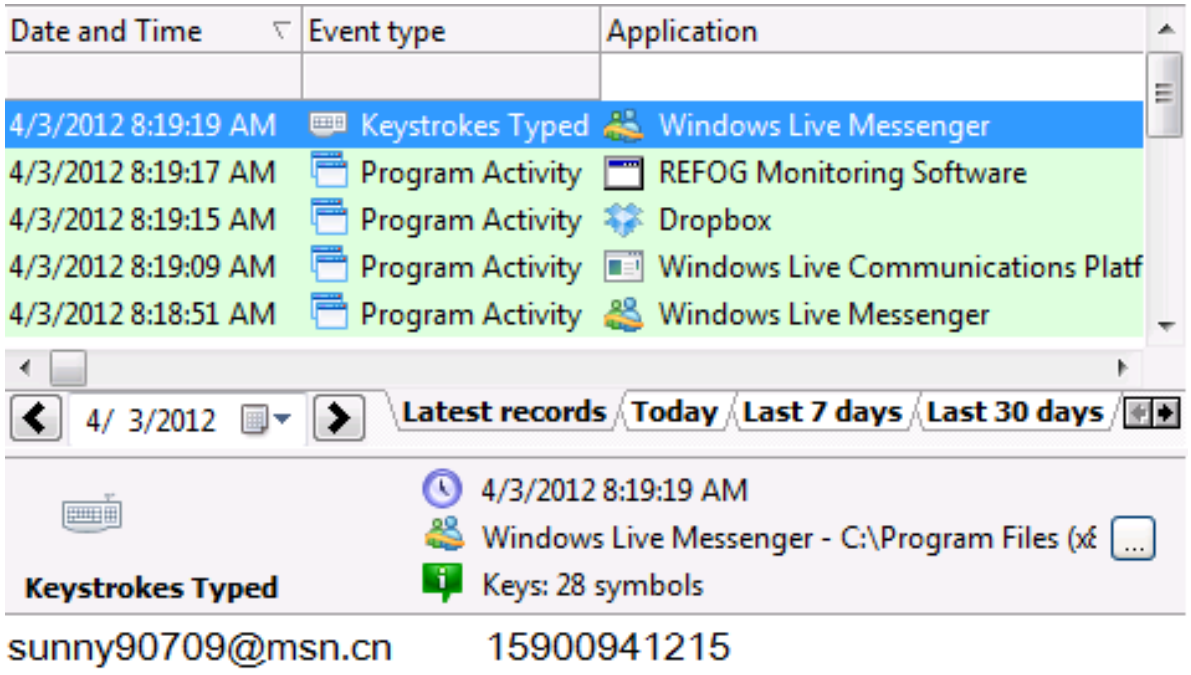


REFOG Free Keylogger configuration

Keylogger

Sign in to Windows Live Messenger

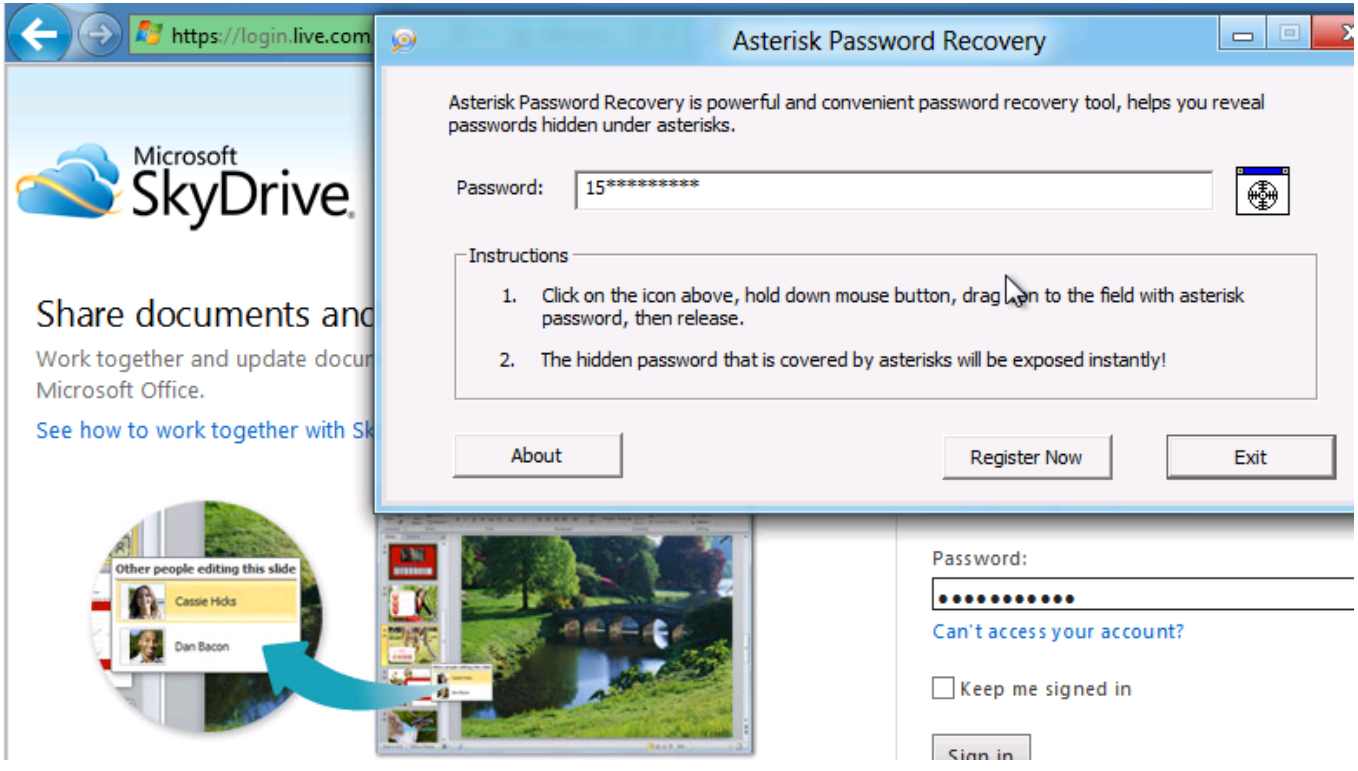
Keylogger



Windows Live ID and password collected by keylogger

Read from text input control

Malware can read password from a text input control, even if it's displayed as asterisks.



Asterisk Password Recovery reads a password from SkyDrive login page

Malware

- Malware can also aid other phishing techniques:
  - for web spoofing
    - install phisher's CA certificate as a trusted root CA, so browser will not show the warning page when visiting a spoofed https website
  - for pharming
    - change the hosts file or DNS settings
    - run ARP spoofing on local Ethernet
  - enlist into botnets
    - send spoofed emails
    - serve forged websites

Countermeasure: client security products

- Client security products are widely deployed
  - Anti-virus products
  - Malicious Software Removal Tool (monthly from Microsoft Update)
- They are not always effective
  - It's easy to modify malware so that it doesn't contain any known signature
  - There are techniques to bypass certain behavior-based detection

Countermeasure from China Merchants Bank

online banking client

+

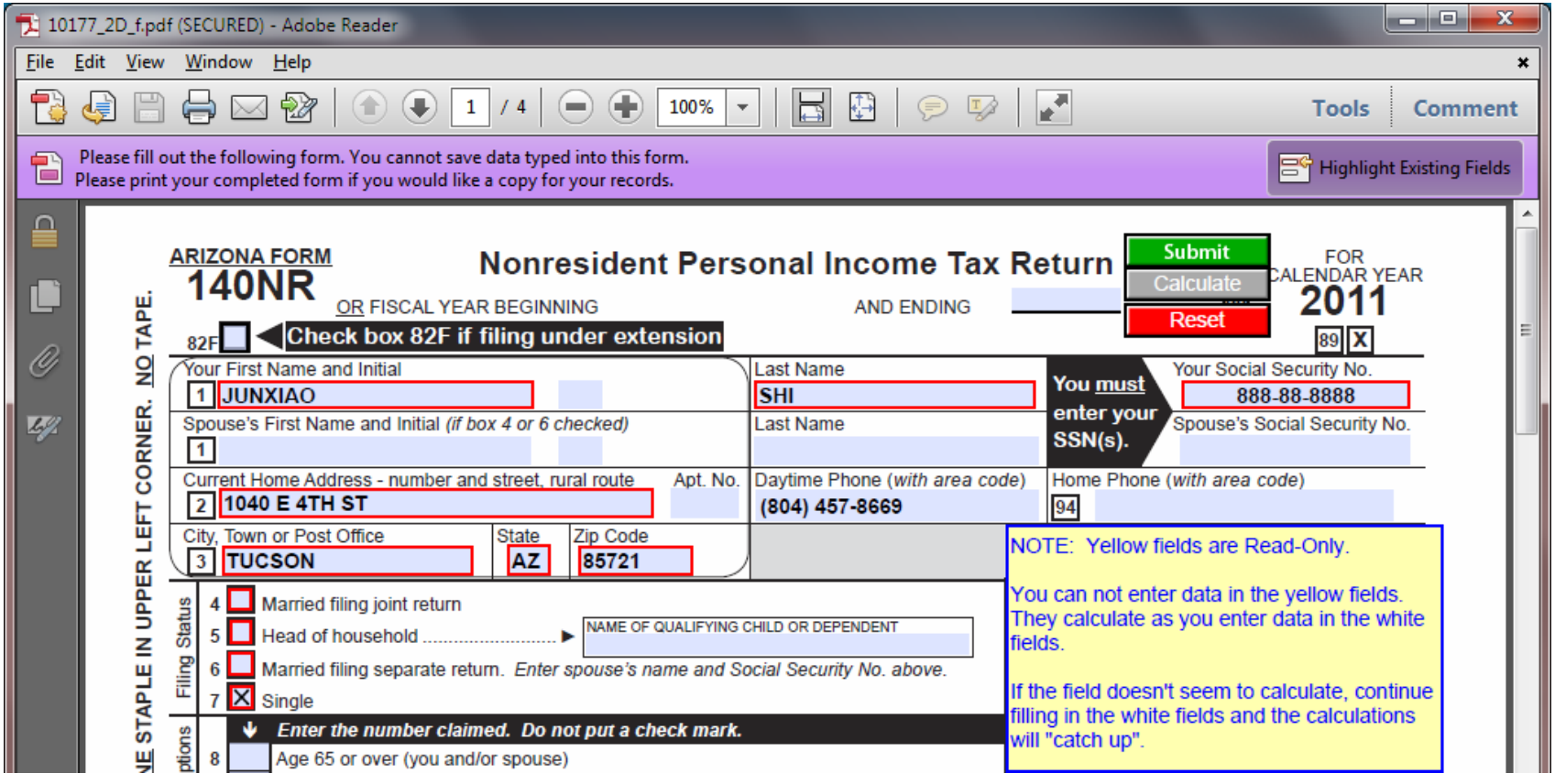
USB token

- secure the text input control, so that (most) keyloggers cannot intercept keystrokes or read its content
- encrypt confidential information in memory and over network
- provide mutual authentication by client and server certificates

Why is this possible

- PDF: Most popular & trusted document description format.
- PDF programming language: Strong execution features which can be exploited.

Illustration



fake tax return form received in a spoofed email

How does it work?

SubmitForm action

- Upon invocation of a SubmitForm action, names and values of selected interactive form fields are transmitted to the specified URL / email.
- Recipient URL or email address is set at the time the form is created.

References: Books

- Jakobsson, M., & Myers, S. (2007). Phishing and countermeasures: Understanding the increasing problem of electronic identity theft. Hoboken, N.J: Wiley-Interscience.
- James, L. (2005). Phishing exposed. Rockland, MA: Syngress.
- ISO 32000-1:2008 Document management – Portable document format – Part 1: PDF 1.7

References: Online Resources

- VeriSign `https://www.verisign.com`
  `https://www.phish-no-phish.com`
- Windows Live SkyDrive `https://skydrive.live.com`

References: Software

- Windows 8 Developer Preview http://msdn.microsoft.com/en-us/windows/apps/br229516
- Windows Live Essentials http://windows.microsoft.com/en-US/windows-live/essentials-home
- REFOG Free Keylogger http://www.refog.com/free-keylogger/key-logger.html
- Asterisk Password Recovery http://www.top-password.com/asterisk-password-recovery.html
- China Merchants Bank personal banking client http://www.cmbchina.com/cmbpb/v36/pb.htm
- Adobe Reader http://get.adobe.com/reader/