

Deter, Detect, Defend



INDUSTRIAL STATE BANK

Deter

- Never provide personal information, including social security number, account numbers or passwords over the phone or Internet if you did not initiate the contact
- Never click on the link in an email if you believe it is fraudulent
- Don't use obvious passwords like your birth date, mother's maiden name or the last four digits of your social security number
- Keep your computers up to date with antivirus software, firewalls



Detect

Be alert to signs that require immediate attention:

- Bills that do not arrive as expected
- Unexpected credit cards or account statements
- Denials of credit for no apparent reason
- Calls or letters about purchases you did not make



Defend

If you fall victim to an attack, act immediately to protect yourself:

- Alert your Online Banking Coordinator
913 831-2000 or
pcbanking@industrialbankkck.com
- Place fraud alerts on your credit files
- Monitor your credit files
- Keep computer safe with up to date antivirus software and firewalls



Phishing

Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic or voice communication.

Be aware if you receive an email that looks like it came from a reputable company. It could direct you to a phony website which may ask you to update your personal information. If you provide this information you may find yourself victim of identity theft.



Pharming

Pharming is the term for criminal hackers redirecting Internet traffic from one website to a different, identical-looking site.

Protect yourself:

- Always use a secure website
- Review your Internet banking often
- Check credit and debit card statements
- Regularly check that your browser is up to date



Spyware

Spyware can be installed on your computer without your consent. It monitors or controls your computer use and may be used to send you pop-up ads, redirect your computer to websites, monitor your Internet surfing or record your keystrokes, which in turn, could lead to identity theft.



Effects of Spyware

- A barrage of pop-up ads
- A hijacked browser
- Sudden or repeated change in your computer's home Internet page
- New and unexpected toolbars
- New and unexpected icons on the system tray at the bottom of your computer screen
- Keys not working
- Random error messages
- System running slowly and anti-virus not updating



Malware

Malware is short for “malicious software;” it includes viruses – programs that copy themselves without your permission.

Computers may be infected with malware if they:

- Slow down, malfunction or display repeated error messages
- Won't shut down or restart
- Serve up a lot of pop-up ads or display them when you're not surfing the web
- Display web pages or programs you didn't intend to use or send emails you didn't write



Dot “Cons”

Con artists have gone high tech, using the Internet to defraud consumers in a variety of ways. According to the FTC, online consumers complain most about the following:

- Internet auctions
- Internet access services
- Credit card fraud
- International modem dialing
- Web cramming
- Multilevel marketing plans
- Travel and vacation
- Business opportunities
- Investments
- Health care products/services



Beware of a Free Security Scan

Messages telling you to install and update security software for your computer seem to be everywhere. You might be tempted by an offer for a “free security scan,” especially when faced with a pop-up, an ad that claims malicious software has already been found on your machine. Unfortunately it’s likely that the alarming message is a scam.



Wireless Network Security Tips

The downside of a wireless network is, unless you take certain precautions, anyone with a wireless-ready computer can use your network.

- Use encryption
- Use anti-virus and anti-spyware software and a firewall
- Turn off identifier broadcasting
- Change the identifier on your router from the default
- Change your router's pre-set password for administration
- Allow only specific computers to access your wireless network
- Turn off your wireless network when you know you won't use it
- Don't assume that public hot spots are secure



Bank Provided Protection

- Multi-factor authentication
- 128 bit encryption
- Customer created password
- Email alerts
- Three failed logon attempts results in lockout
- Timeout feature



Bank Provided Protection

A bank representative would only contact you if:

- An online bill payment failed
- Your email address needed to be verified
- You were locked out of online banking



Your Responsibilities

- Install anti-virus software on your computer and keep it up to date
- Scan your computer routinely for viruses
- Monitor your account(s)
- Do not write your password down or save it in a Word document
- Notify the bank if you believe your computer has been compromised, i.e. unauthorized transfers or misplaced passwords



Your Responsibilities

In addition to the previously referenced recommendations, commercial customers should periodically perform a related risk assessment and control evaluation.



Bank Contact Information

Notify Industrial State Bank if you have any concerns about your account.

Online Banking Coordinator – **913 831-2000** or
pcbanking@industrialbankkck.com



Additional Resources

- <http://onguardonline.gov/articles/0003-phishing>
- <http://onguardonline.gov/articles/0002-common-online-scams>
- http://www.ftc.gov/multimedia/video/phishing/phishing-scams_eileen.shtm
- <http://consumerprotection.uslegal.com/phishing/>

