Cybersecurity: Protecting Your Agency From Cybercrime

Commonwealth of Virginia Information Security Conference
April 12, 2018

2017 Was the Year of the Bombshell Hack

Hackers managed to cause chaos at global companies, swiped half of all Americans' Social Security numbers, and boosted the cyber insurance market.

What is cybercrime?

Cybercrime is criminal activity involving the internet, a computer system, or computer technology.

50% of online adults

About half of online adults were cybercrime victims in the past year.

$500 billion

Cybercrime costs the global economy up to $500 billion annually.

20% of businesses

One in five small and medium businesses have been targeted.

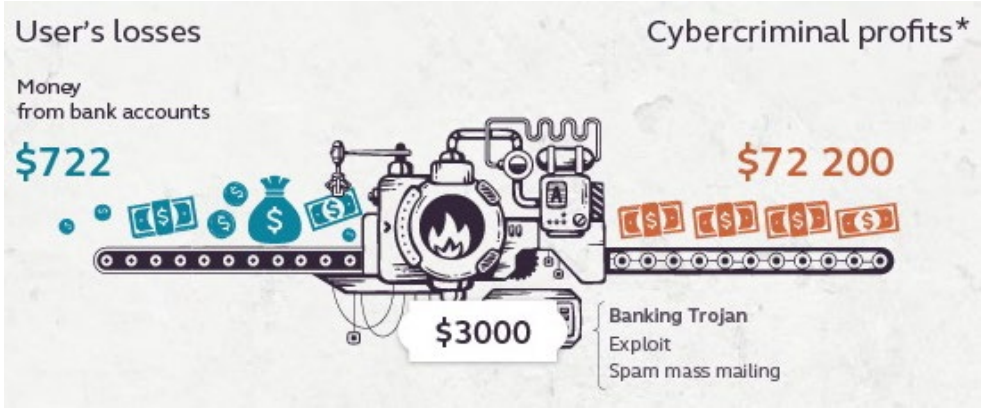
93 percent of all money is digital. That's what is at risk here. –Bill Nelson

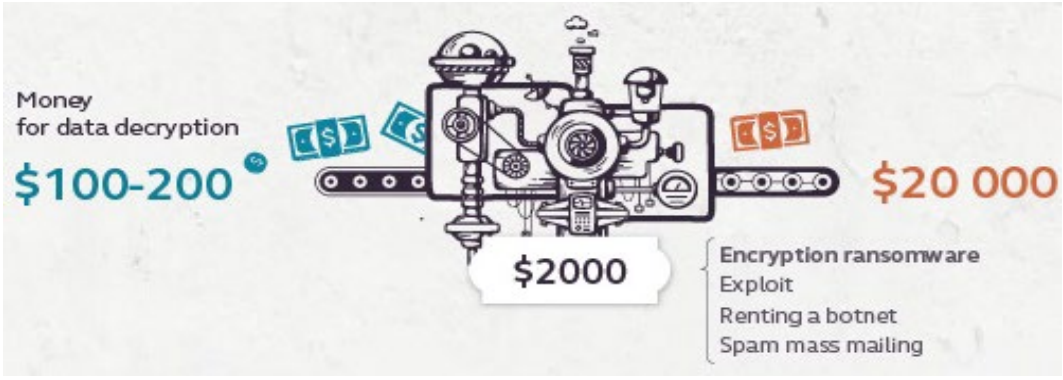
Bill Nelson, Financial Services Information Sharing & Analysis Center

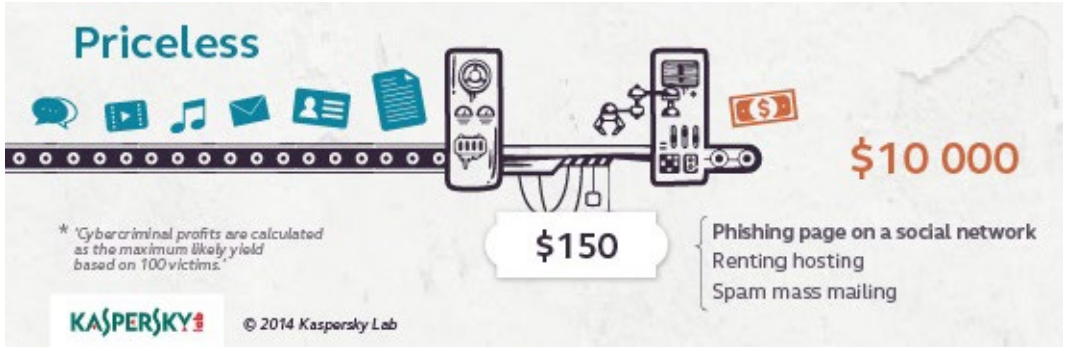
Financial impact of cybercrime

- One large company breached per month
- Many small to medium sized companies are breached per week

Key ways that hackers earn money







Cybercrime is big business.

Cybercrime activity is at the highest, ever

Cybercrime is more organized and motivated than at any time in history. The blackhat cybercriminal is a professional adversary.

This industry has evolved with the evolution of the internet and opportunities associated with PC/computer/mobile devices.

Insights about one group of three Blackhats recently indicted:

- Stole information on 100 million people
- Breached 12 companies, including

JPMorgan E*TRADE DOWJONES

- Earnings at over $100 million
- Employed 270 employees in Ukraine and Hungary in just one of their illicit businesses

http://www.reuters.com/article/us-hacking-indictment-idUSKCN0SZ1VM20151110

What is **Blackhat** cybercrime?

Blackhat cybercrime is a form of malicious online behavior motivated by *profit* and a *predictable ROI*

- Understanding Blackhat criminal *tools, techniques, motivations, cultures*, and *ecosystems* are critical to defending against current attacks and deterring future ones

- Treating Blackhat cybercrime as a purely technological problem makes mitigation difficult and costly

The bad actors are not a monolithic group

Script-kiddies

- Non-professional cybercriminals
- Use crime kits to make spending money
- Little to no business or technical expertise
- Even though they are not professional, their impact can be significant

Grayhats

- They believe they are offering legitimate services. However, their customers can be both "legitimate" or criminal
- Ran as a business

Blackhats

- Treat cybercrime as a business
- Business and technical expertise
- Often work in a closed group of other professional cybercriminals
- Criminal reputation is everything

State Sponsored

- National security and/or economic motivation
- Technical expertise
- Work in a closed group of other professionals
- Often use Blackhat resources and/or techniques to mask their identity

Hactivists

- Individuals or groups who hack for a social cause, without economic motivation
- Have both technical people and followers

Some elite Blackhats, some elite hactivists, and most state sponsored actors use "APT" techniques

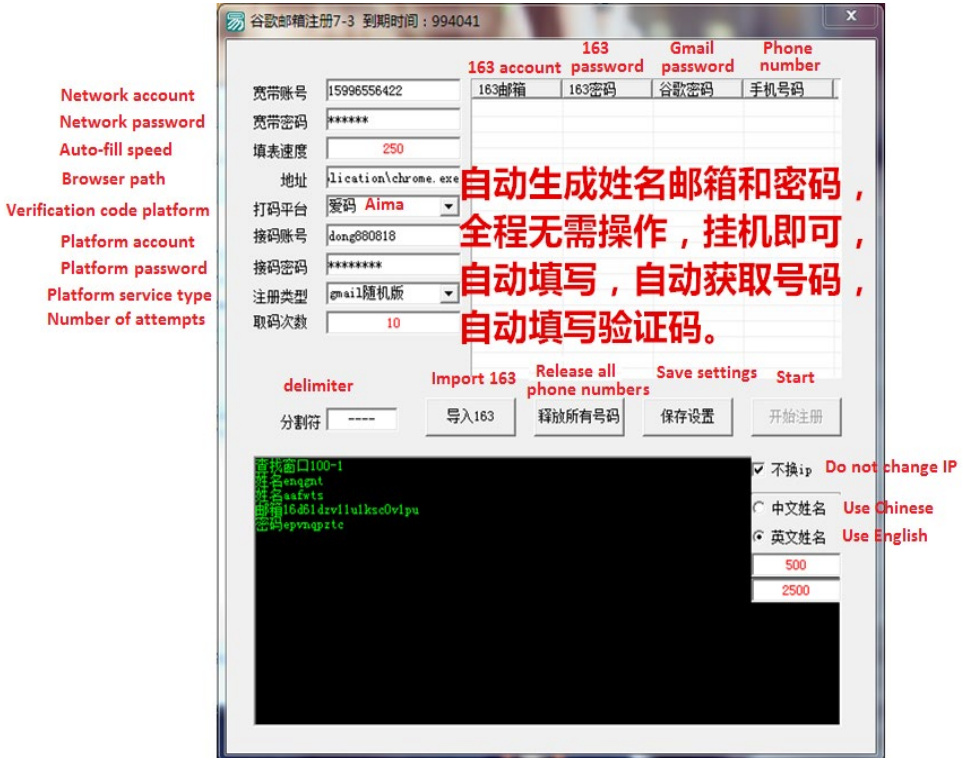
The cybercrime problem is broad, and getting worse

- More professional cybercrime services make it easier for would-be attackers to become cybercriminals
  - Many cybercriminals don't need technical abilities when entering the world of cybercrime
- In many regions, it is socially acceptable to steal from victims on the Internet
- The line is blurring between state sponsored attackers and cybercriminals
  - Elite teams of attackers that have the same resources, skills, and patience as state actors

It has never been easier for new entrants into the market

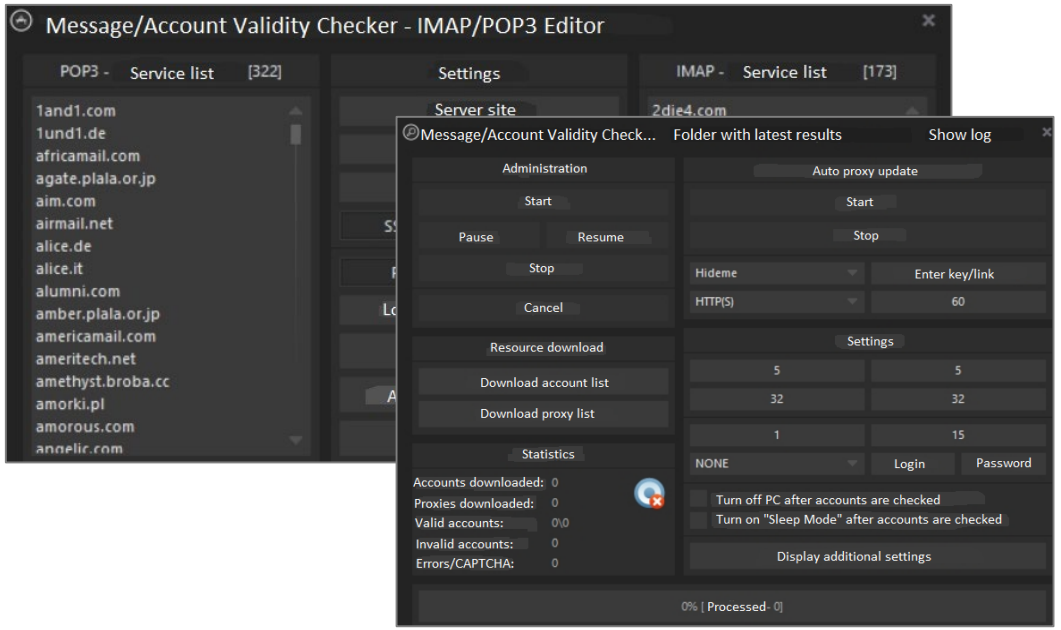
Cybercrime as a Service (CaaS): Crimekits and services available

Tools to create abuse accounts



Chinese **Gmail account creation tool**, interfaces with SMS and CAPTCHA solving services

Account Checkers

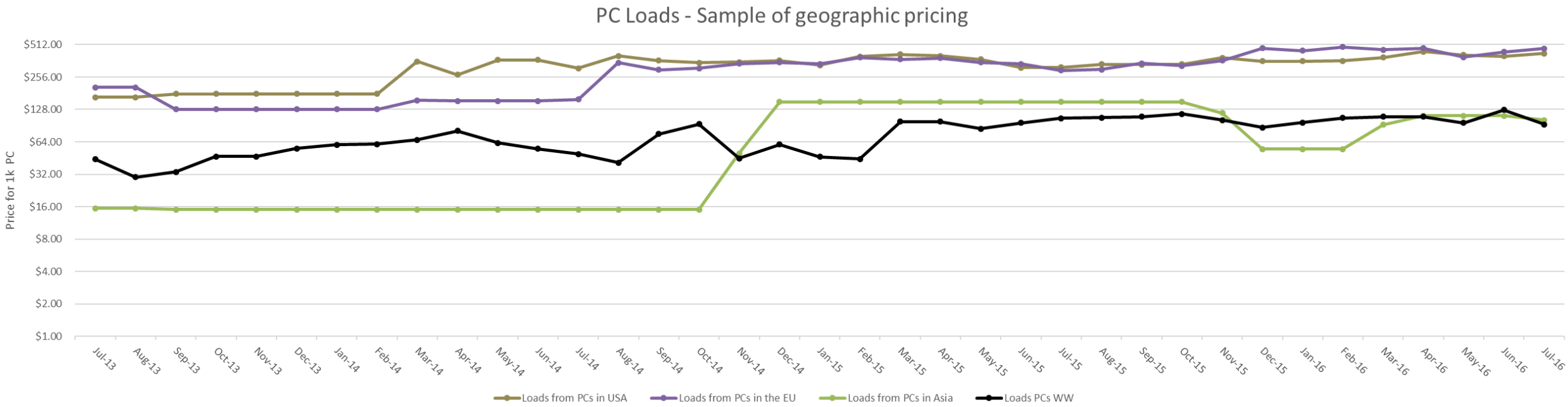


Russian checker **Private Keeper**. It is a universal checking tool supporting 17 different web services (PSN, PayPal, Skype, Twitter, etc.) and many email providers. It has an IMAP/POP3 server editor that supports "almost any email service" and allows users to parse the content of messages and check email accounts validity

Sources: Various

It has never been easier for new entrants into the market

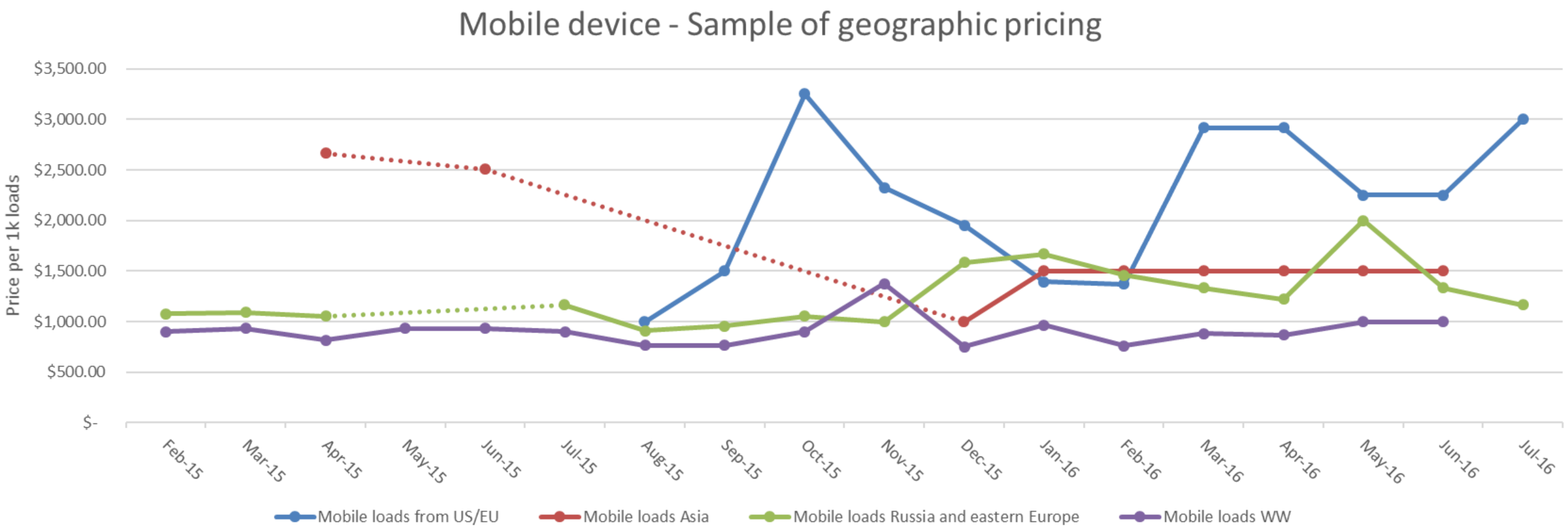
Cybercrime as a Service (CaaS): Market for freshly infected PCs to push malware to



Sources: Various

It has never been easier for new entrants into the market

Cybercrime as a Service (CaaS): Market for freshly infected mobile devices to push malware to



Sources: Various

How kits are used

Botnet

- A botnet is a network of devices infected with malicious software that is centrally controlled
- “Good” malware cannot be detected by users

Phishing

- Campaigns can include spam, SMSishing, Vishing, etc.
- The intent is to trick the user into giving up their password, account recovery information, or PII

Ransomware

- It holds your PC or files for "ransom.”
- Prevents you from using your PC
- Victim has to pay to regain access

Considerations when combating cybercrime

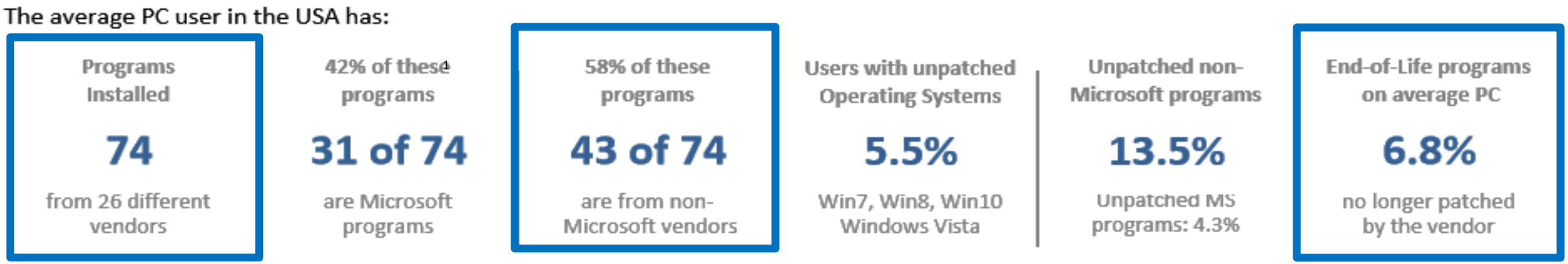
To be successful in cyber defense, one needs to know what are effective and durable mitigations

- Defenders must not rely on your users doing the right thing at the right time
- Be proactive, prevent the attack, and prevent the attacker from predicting their ROI
  - This can include monitoring for their probes and enabling defensive measures to act between their probes and attack

Tips to keep your agency safe

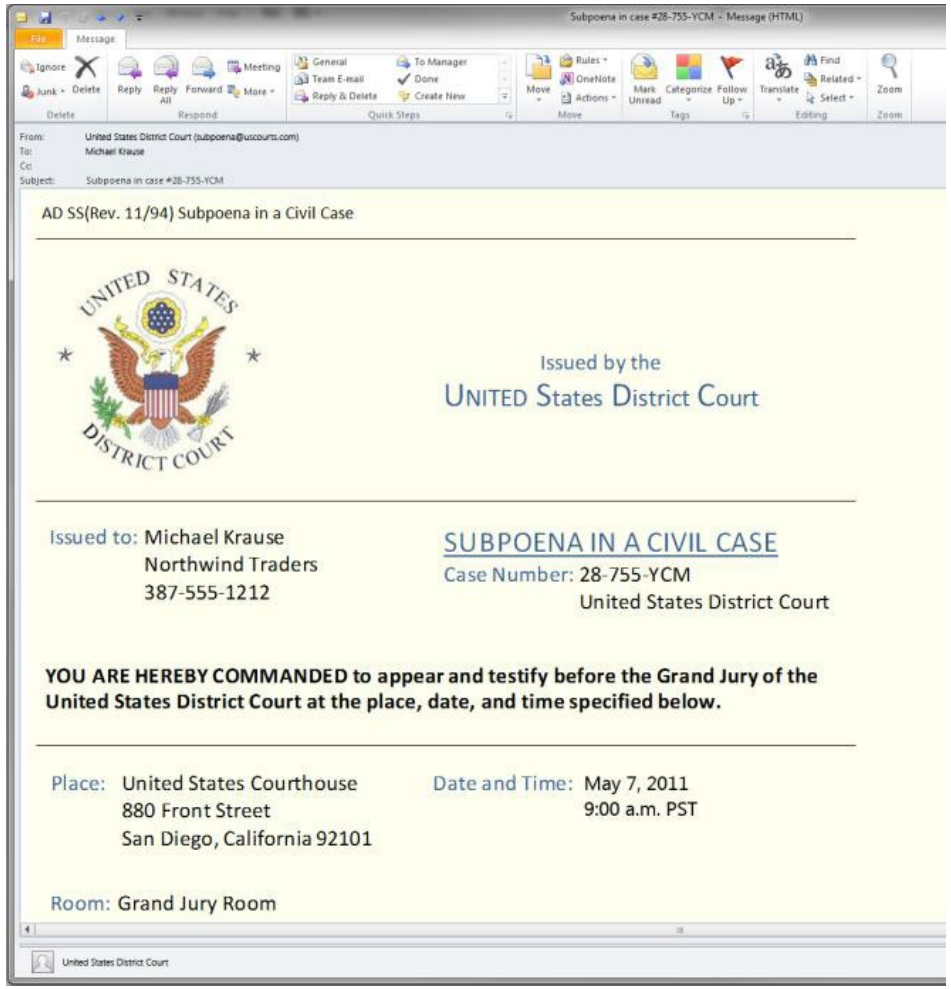
1. Strengthen your computer's defenses

- Keep the firewall on (work, home, public networks)
- Install legitimate anti-malware software (http:/aka.ms/wkactd)
- Keep software up to date (automatically)

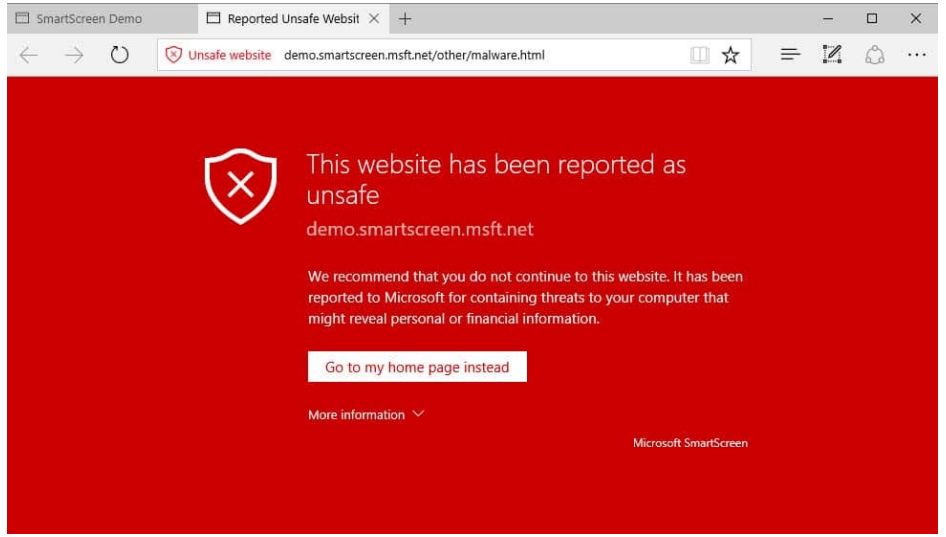


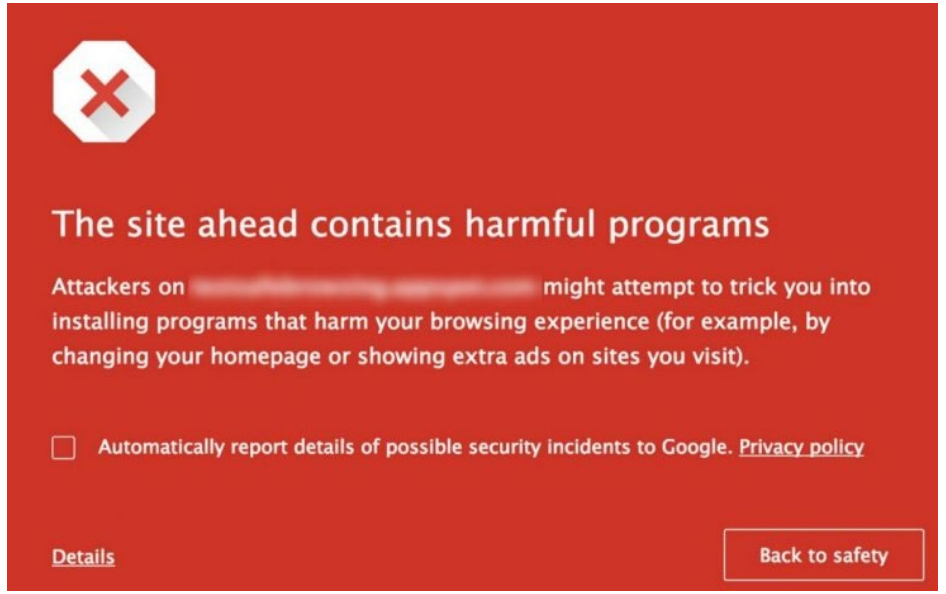
[1] statistics noted from Flexera software

2. Don’t be tricked into downloading malware



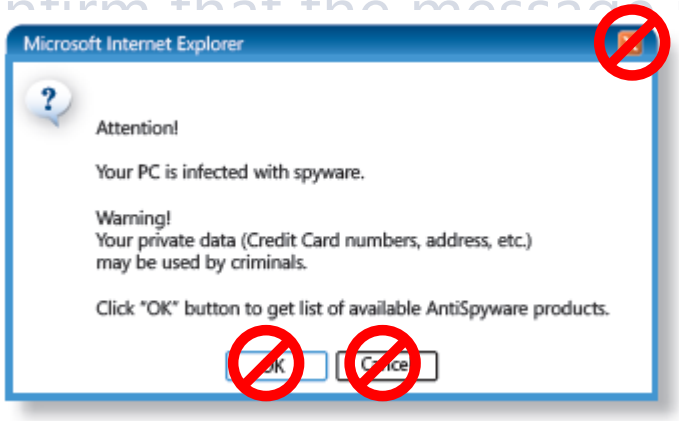
- Train your users to use malware and phishing protection in their browsers.
- Keep antivirus on and updated





2. Don’t be tricked into downloading malware

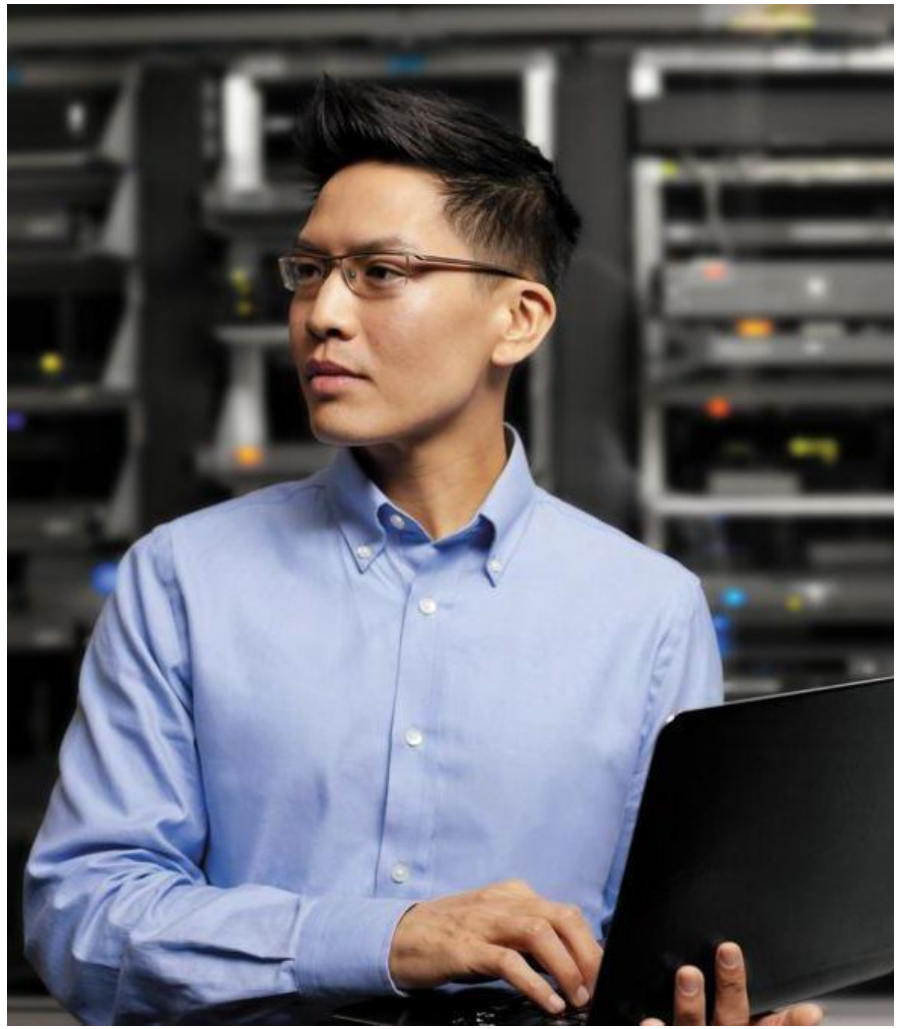
- Think before you click
- Confirm that the message is legitimate
- Close carefully



Step 2

3. Protect company data and financial assets

- Encrypt confidential data
- Use rights management solutions to handle sensitive data
- Train your users to identify scams and fraud
- Use HoneyTrap accounts in your domain. Notify on successful and unsuccessful logins
- Use HoneyTrap documents. Notify on successful and unsuccessful access



3. Protect company data and financial assets

How to evade scams

Look for telltale signs

- Think before you click

www.snopes.com

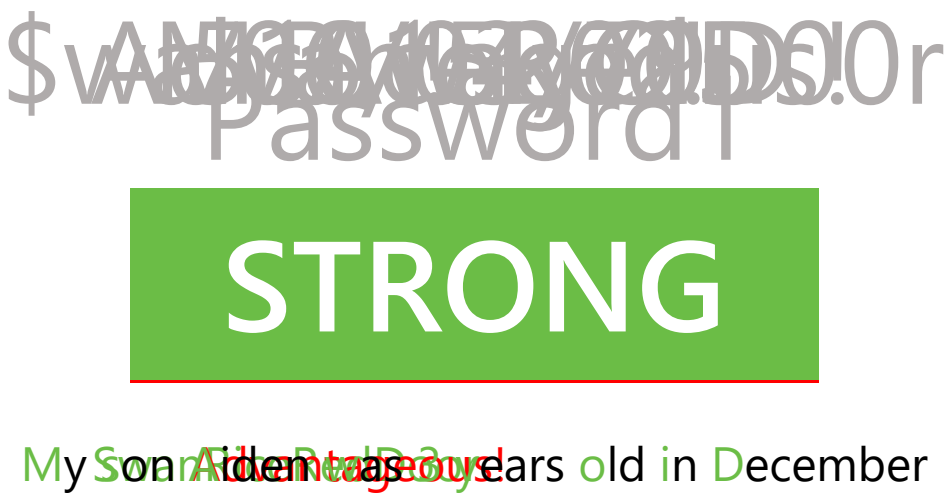
Keep sensitive information private

Train employees to identify socially engineered attacks

4. Passwords. Keep them strong, private, and don’t reuse them

4. Passwords. Keep them strong, private, and don’t reuse them

Guess which
passwords are strong?



4. Passwords. Keep them strong, private, and don’t reuse them

Protect your accounts and passwords

- Make passwords strong (still needed)
- Keep them private (don’t share among users)
- Use unique passwords for different websites
- Limit use of employees using corporate e-mail accounts as their identifier on third-party website

Defend against checkers

- Enable disabling accounts on too many invalid login attempts
- Don’t use insure interfaces (e.g. unprotected POP/IMAP/SMTP)
- Monitor for brute force and snowshoe checkers

5. Guard data and devices when you're on the go

5. Guard data and devices when you're on the go

- Connect securely
- Confirm the connection
- Encrypt storage on mobile devices
- Save sensitive activities for trusted connections
- Flash drives: watch out for unknowns and disable auto run
- Enable features like Work Folders and cloud storage to manage work data on mobile devices

5. Guard data and devices when you're on the go

What to do if there are problems

- Have a predefined process and checklist to identify company identities, data, services, and applications on the device
- Report abuse and other problems
- Immediately report phishing
- Immediately report missing devices or theft of company data
  - Change all passwords
  - Wipe mobile phones

Let’s assess your security risk

Use this interactive risk assessment tool to select all threats your company might face and estimate the cost of each. This worksheet will then calculate the total cost and provide countermeasures you can take to protect your company.

http://aka.ms/knowyourrisk

Time: 10 min

AIS Network

Managed Security Services