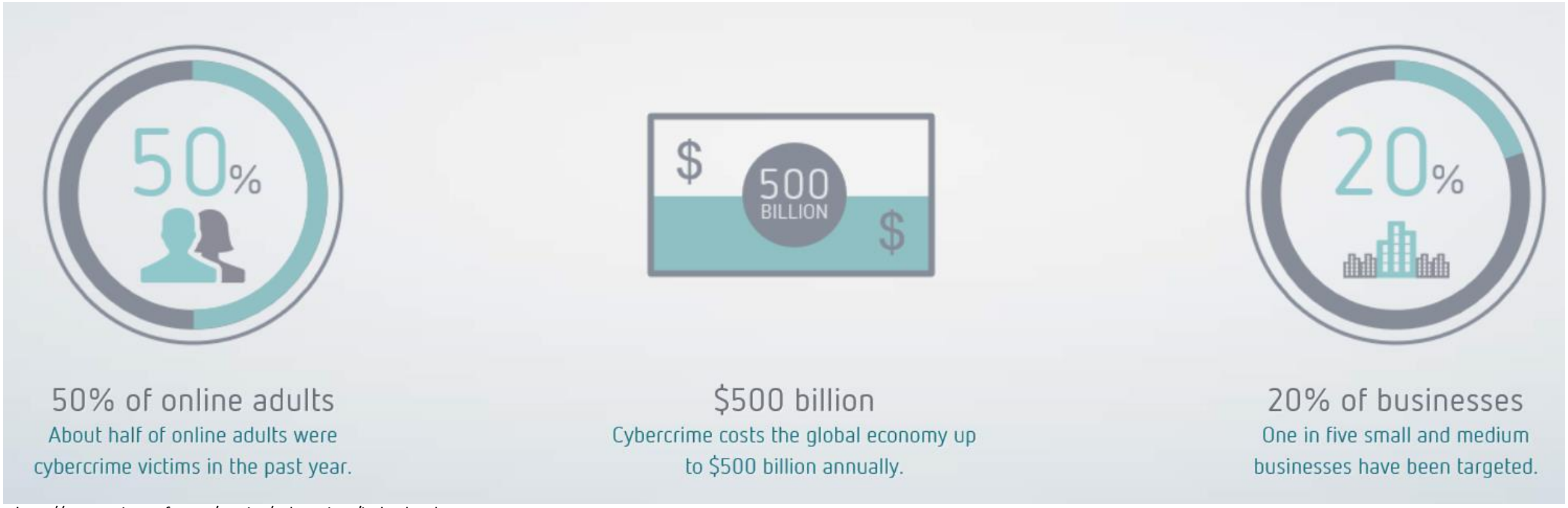
Cybersecurity 101: Protecting Your Business from Cybercrime

What is cybercrime?

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



http://news.microsoft.com/stories/cybercrime/index.html

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

Bill Nelson, Financial Services Information Sharing & Analysis Center

The bad actors are not a monolithic group

Often defenders treat all bad actors the same

Non-Professional

- 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

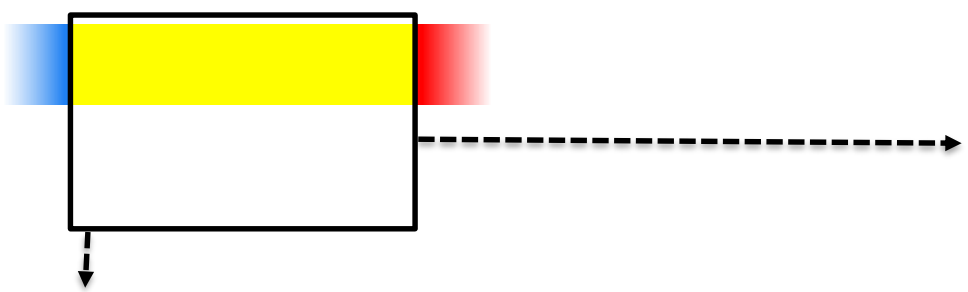
Hactivists

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

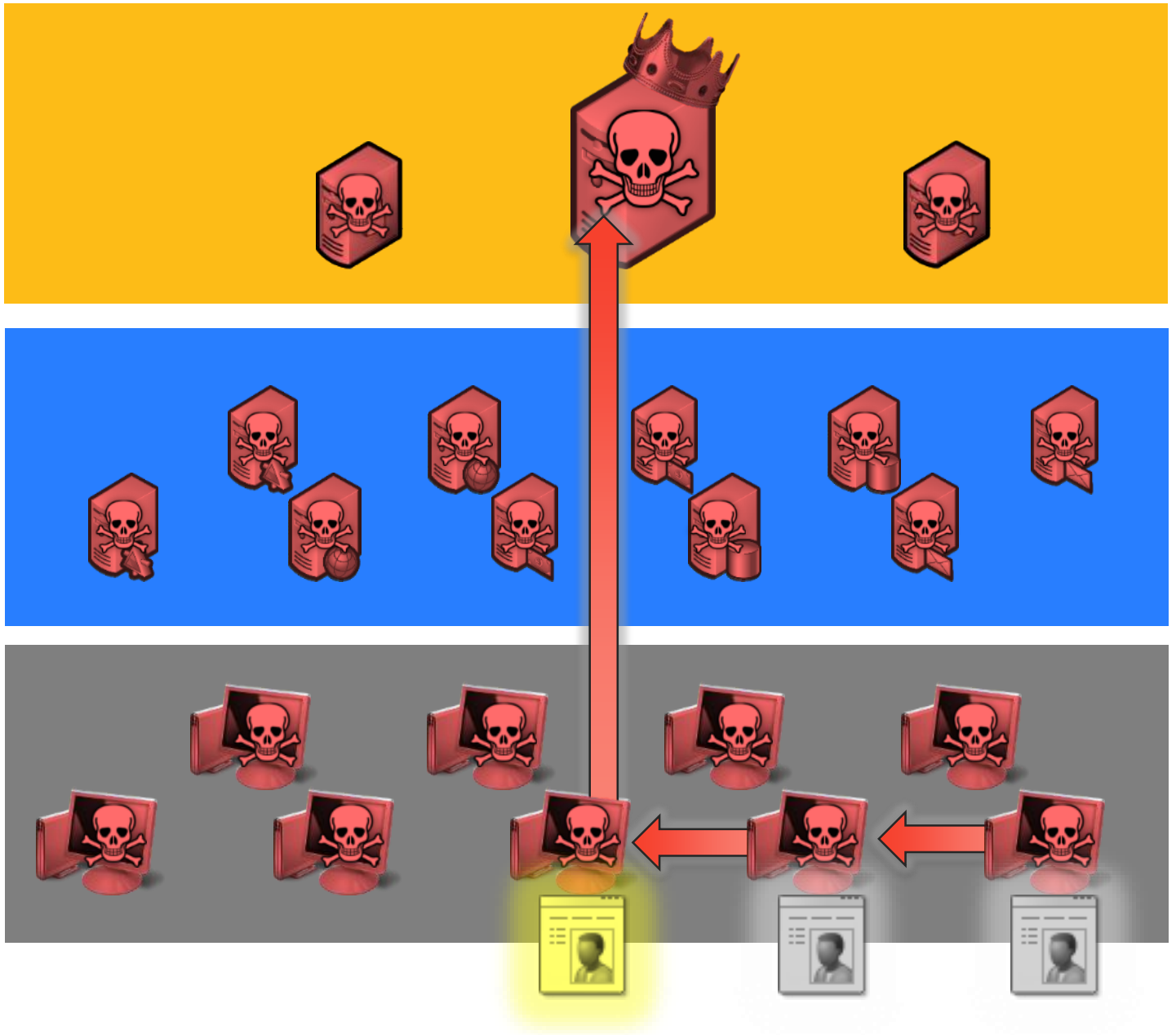
Tools, techniques, motivations, and business models vary by cybercriminal region

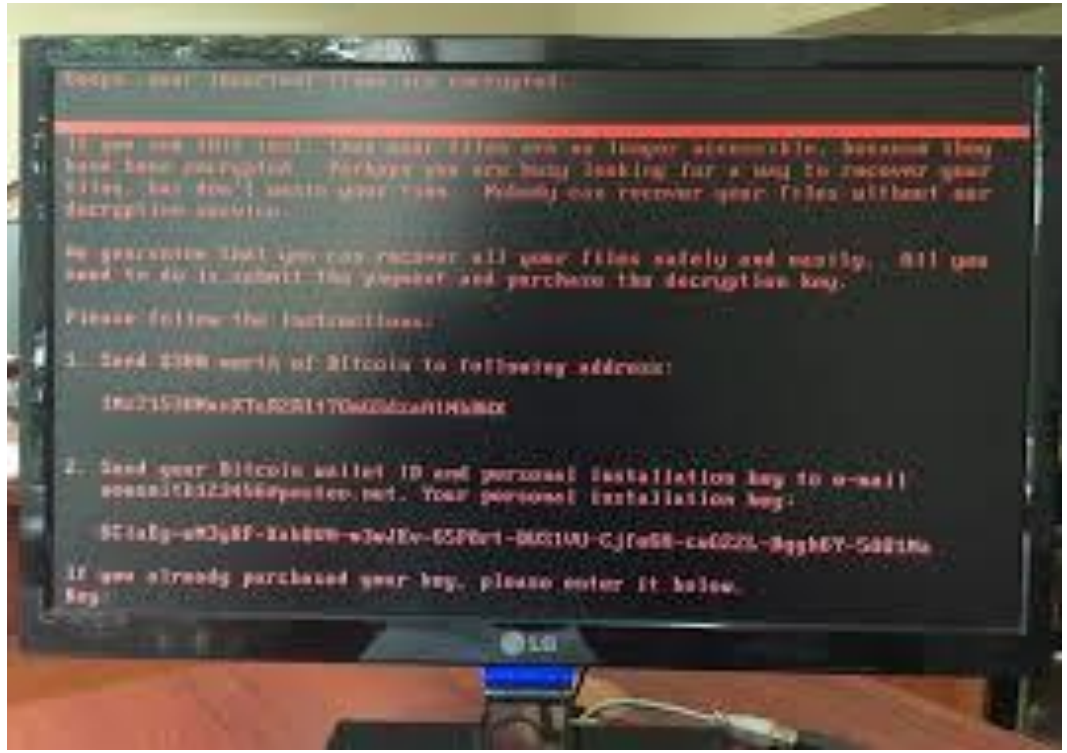
Some elite Blackhats, some elite hactivists, and most state sponsored actors use "APT" techniques

Privilege Escalation with Credential Theft (Typical)



1. Get in with Phishing Attack (or other)
2. Steal Credentials
3. Compromise more hosts & credentials (searching for Domain Admin)
4. Get Domain Admin credentials
5. Execute Attacker Mission (steal data, destroy systems, etc.)





Boogs, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

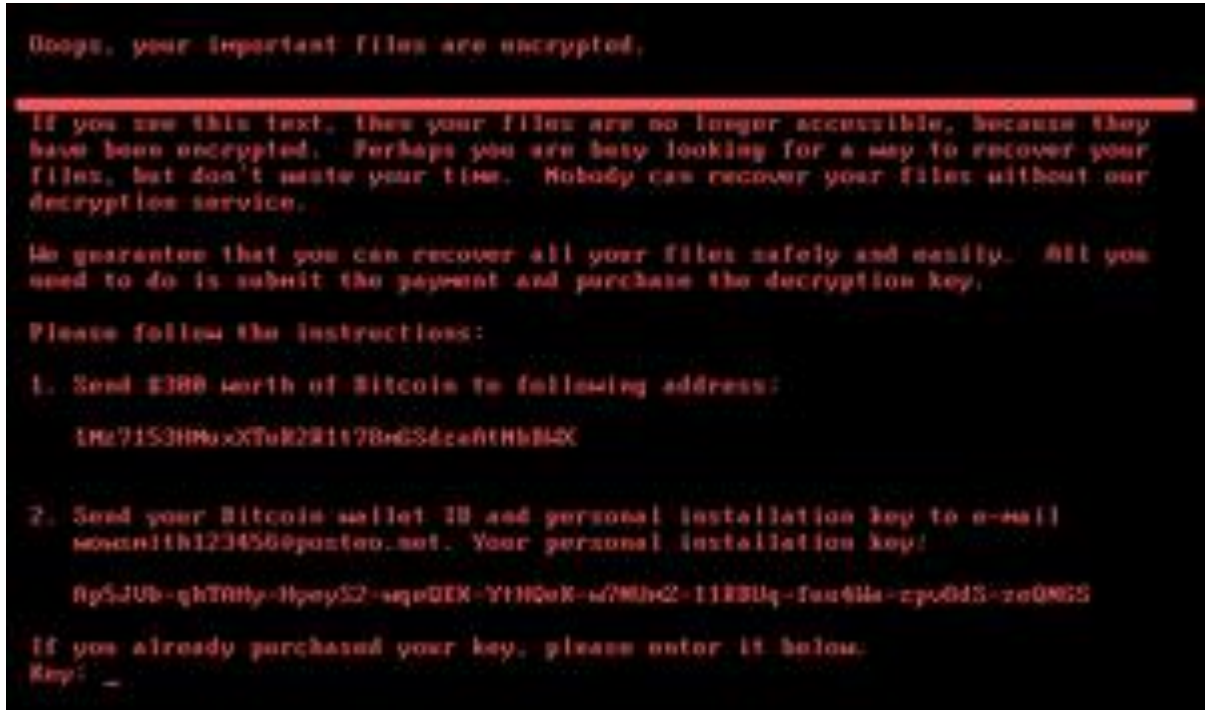
1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wonsmith1234560postoo.net. Your personal installation key:

   8CiaEg-uMJgRF-BxkBVH-mJwJEv-6SPBrt-DUCtVU-GJfmSB-caGQZL-BggbEY-5BBiMa

If you already purchased your key, please enter it below.
Key:



Boogs, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wonsmith1234560postoo.net. Your personal installation key:

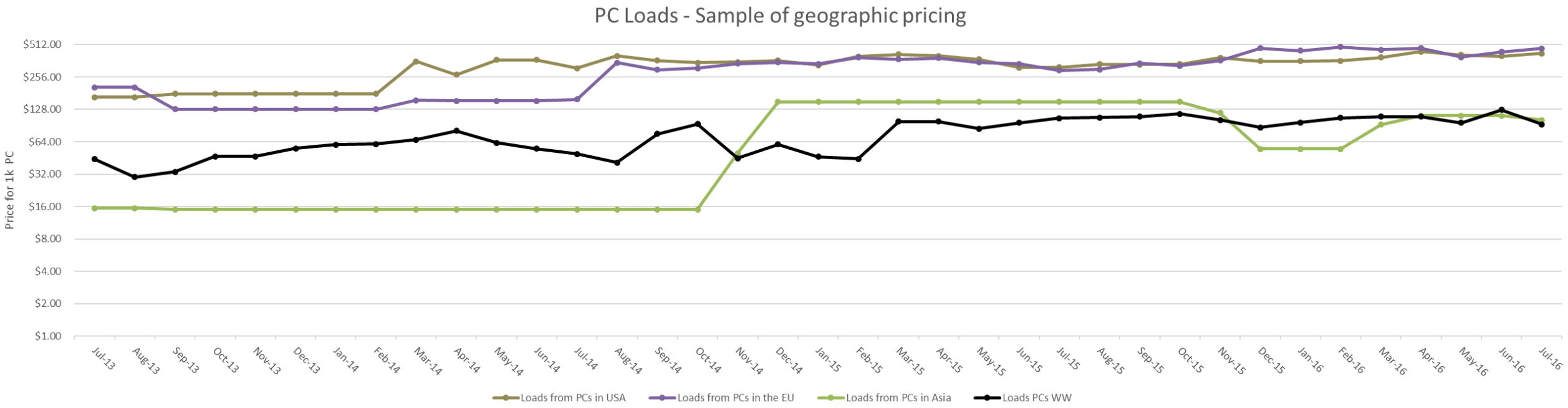
   8pSJUb-ghTRHy-HpeyS2-wqeDEK-YtHQeK-w7MUeZ-tIRBUq-fau4Ue-zpv0dS-zeDMCS

If you already purchased your key, please enter it below.
Key: _

CaaS

It has never been easier for new cybercriminals to start

Market for freshly infected PCs to push malware to

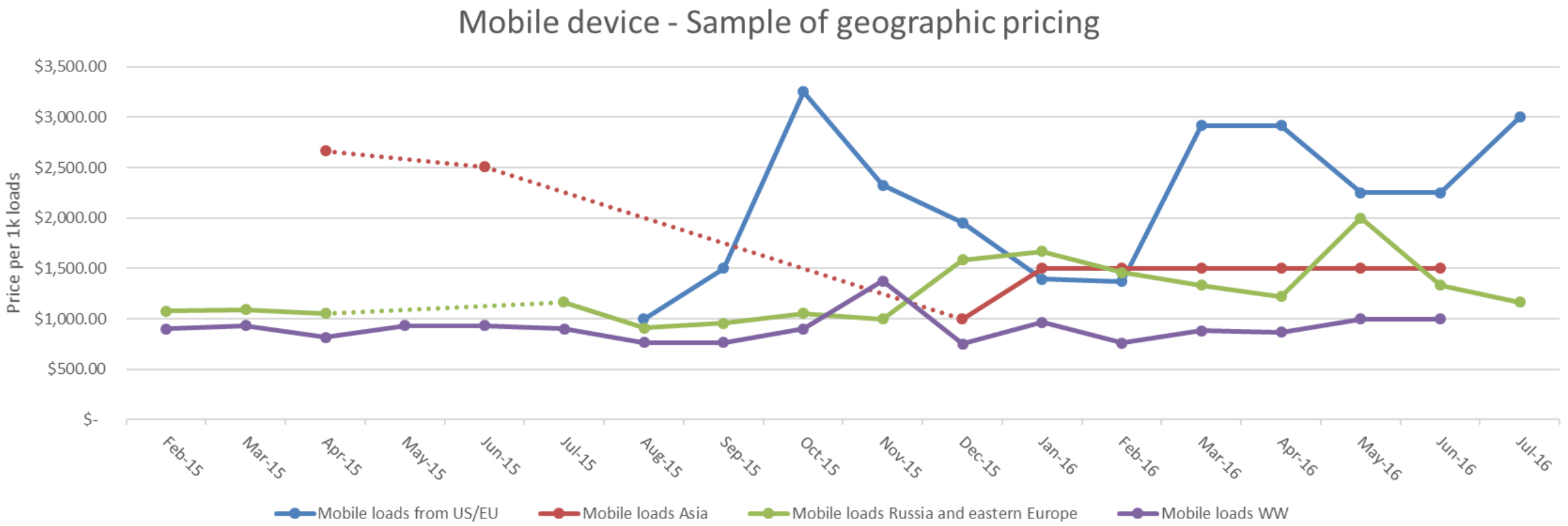


Sources: Various

CaaS

It has never been easier for new cybercriminals to start

Market for freshly infected mobile devices to push malware to



Sources: Various

Cybersecurity Reference Architecture

Microsoft

Vulnerability Management

Security Operations Center (SOC)

Incident Response

Investigation and Recovery

Logs & Analytics

Managed Security Provider

UEBA

Analytics

SIEM

ATA

OMS

Active Threat Detection

Hunting Teams

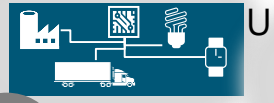
PADS

Enterprise Threat Detection

Security Development Lifecycle (SDL)

80% + of employees admit using non-approved SaaS apps for work (Stratecast, December 2013)

Internet of Things



Unmanaged & Mobile Clients

Software as a Service

box dropbox G salesforce now ...

Office 365

ASM

Lockbox

Identity & Access

Azure Active Directory

Information Protection

Cloud App Security

Conditional Access

Intune MDM/MAM

Azure AD Identity Protection

Azure AD PIM

Multi-Factor Authentication

Hello for Business

MIM PAM

ATA

Active Directory

ESAE Admin Forest

Certification Authority (PKI)

Office 365 DLP

Azure Information Protection (AIP)

- Classify
- Label
- Protect

Hold Your Own Key (HYOK)

Classification Labels

Structured Data & 3rd party Apps

Endpoint DLP

Windows Info Protection

On Premises Da

NGFW

Edge DLP

SSL Proxy

IPS

Office 365 ATP

- Email Gateway
- Anti-malware

Extranet

Colocation

Express Route

Security Appliances

VPN

SIEM Integration

Microsoft Azure

Azure Security Center

- Threat Protection
- Threat Detection

Azure Key Vault

Azure App Gateway

Azure Antimalware

Network Security Groups

...

SQL Encryption & Firewall

Disk & Storage Encryption

DDoS attack mitigation

Backup and Site Recovery

Enterprise Servers

Shielded VMs

VMs

VMs

Domain Controllers

Windows Server 2016 Security

Shielded VMs, Device Guard, Credential Guard, Just Enough Admin, Hyper-V Containers, Nano server, ...

VPN

Privileged Access Workstations (PAWs)

Managed Clients

Sensitive Workloads

IoT

Mac OS

Legacy Windows

Windows 10

EDR - Windows Defender ATP

EPP - Windows Defender

System Center Configuration Manager + Intune

Windows 10 Security

- Secure Boot
- Device Guard
- Application Guard
- Credential Guard
- Windows Hello
- Device Health Attestation
- Remote Credential Guard

Nearly all customer breaches that Microsoft's Incident Response team investigates involve credential theft

63% of confirmed data breaches involve weak, default, or stolen passwords (Verizon 2016 DBR)

Last updated March 2017 – latest at http://aka.ms/MCRA

How kits are used

There are many monetization strategies

Botnets/Malware

- A botnet is a network of devices infected with malicious software that is centrally controlled
- Malware is malicious software that takes advantage of the user, device, and/or network

Phishing

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

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 Cyberdefense, 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 Business Safe

Strengthen your computer's defenses

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

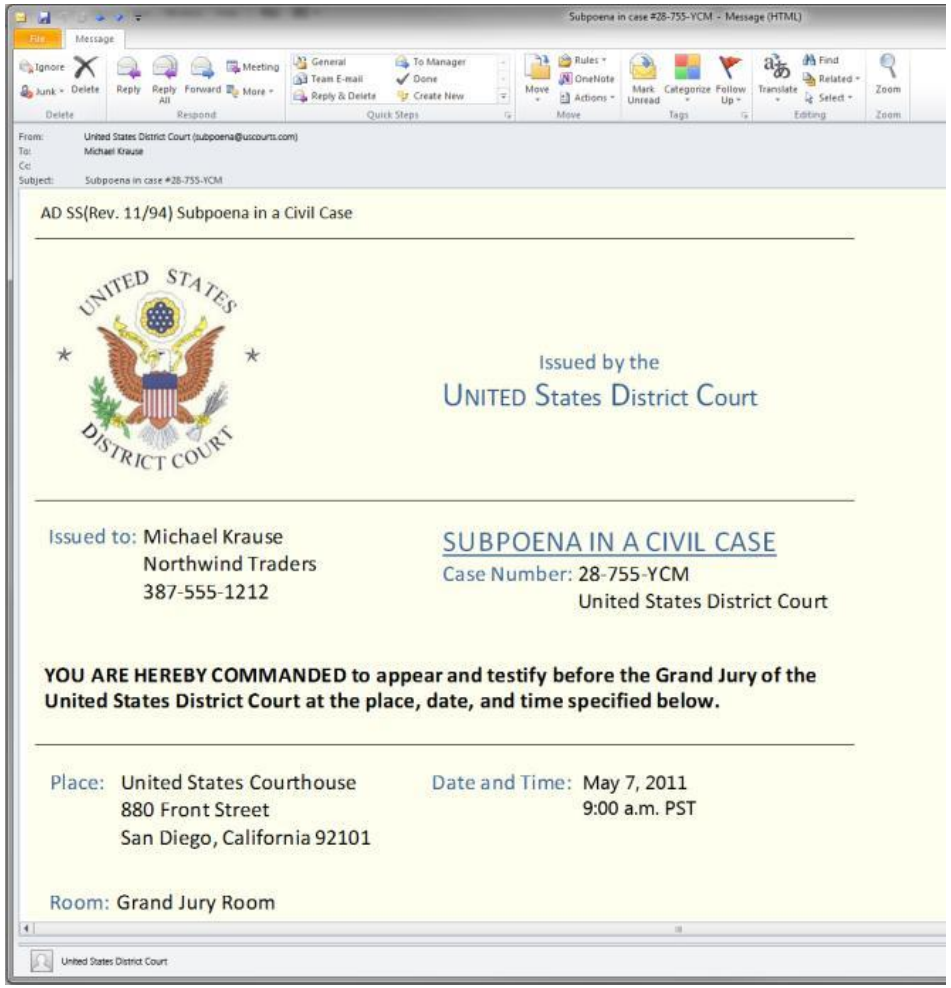
The average PC user in the USA has: [1]

Programs Installed	42% of these programs	58% of these programs	Users with unpatched Operating Systems	Unpatched non-Microsoft programs	End-of-Life programs on average PC
74	**31 of 74**	**43 of 74**	**5.5%**	**13.5%**	**6.8%**
from 26 different vendors	are Microsoft programs	are from non-Microsoft vendors	Win7, Win8, Win10 Windows Vista	Unpatched MS programs: 4.3%	no longer patched by the vendor

Step 1

[1] statistics noted from Flexera software

Don’t be tricked into downloading malware



AD SS(Rev. 11/94) Subpoena in a Civil Case

Issued by the
UNITED States District Court

Issued to: Michael Krause
Northwind Traders
387-555-1212

SUBPOENA IN A CIVIL CASE
Case Number: 28-755-YCM
United States District Court

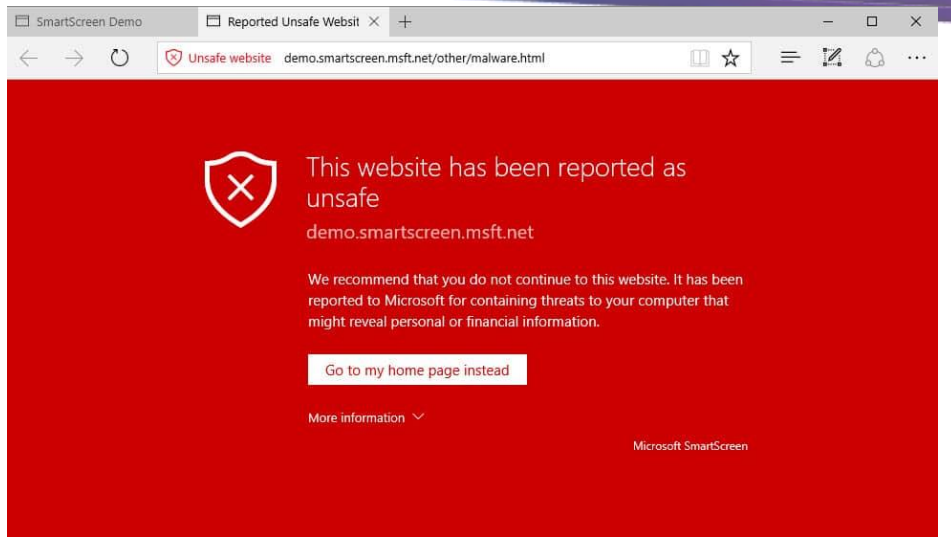
YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

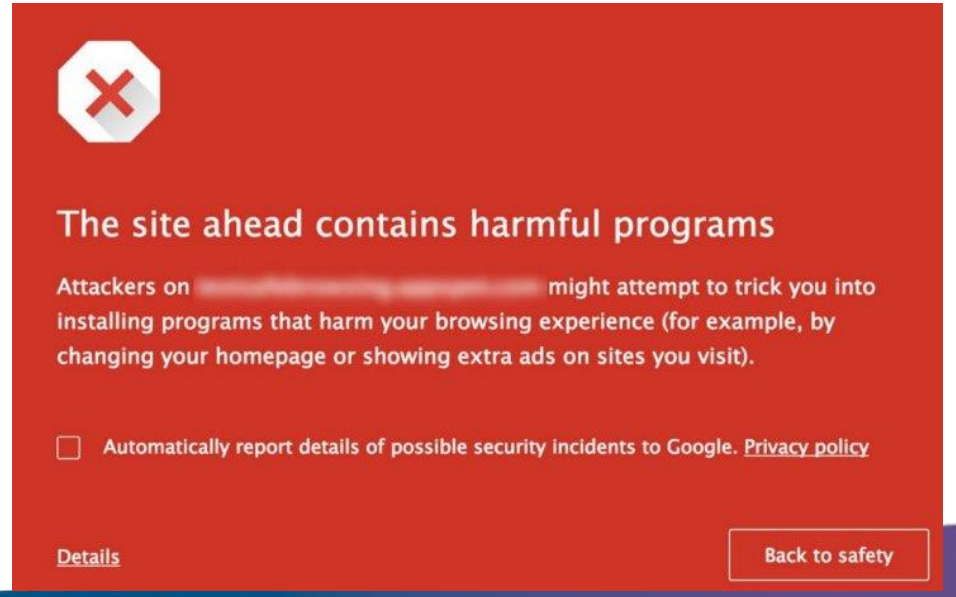
Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7, 2011
9:00 a.m. PST

Room: Grand Jury Room

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

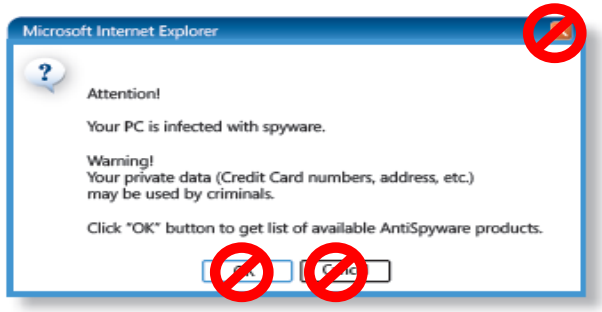




Step 2

Don’t be tricked into downloading malware

- Close pop-up m



Ctrl F4

Step 2

Step 3

Protect company data and financial assets

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

Step 3

How to evade scams

- Look for telltale signs www.snopes.com
- Think before you click
- Keep sensitive information private
- Train employees to identify socially engineered attacks

Step 3

Step 4

Create strong passwords

Keep them private

Don’t reuse them

Create strong passwords

Which passwords are strong?

$vAb...0r

STRONG

My Son Aiden was 3 years old in December

Step 4

Strong passwords are not enough

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 compromised account checkers

Step 4

Step 5

Guard data and devices when you're on the go

Guard company data when you're on the go

- Connect securely
  - Save sensitive activities for trusted connections
- Confirm the connection HLTONHOTELS.NET
- Encrypt storage on mobile devices
- 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

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

Защищенная корпоративная сеть

Що забули?

- Де архіви?
- Як встановлювати
- Як тестувати