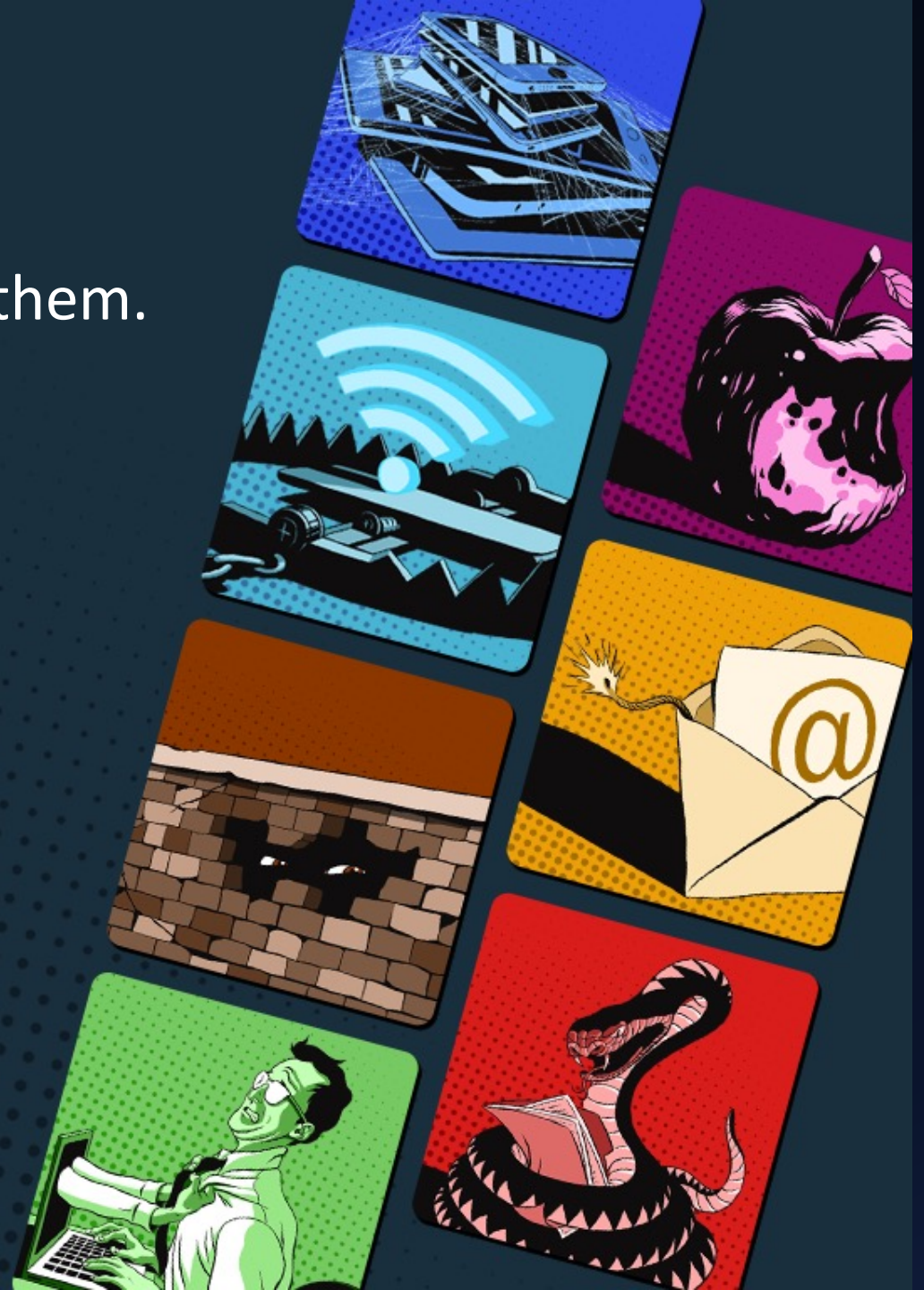
THE 7 DEADLY I.T. SINS



What are Deadly IT Sins?

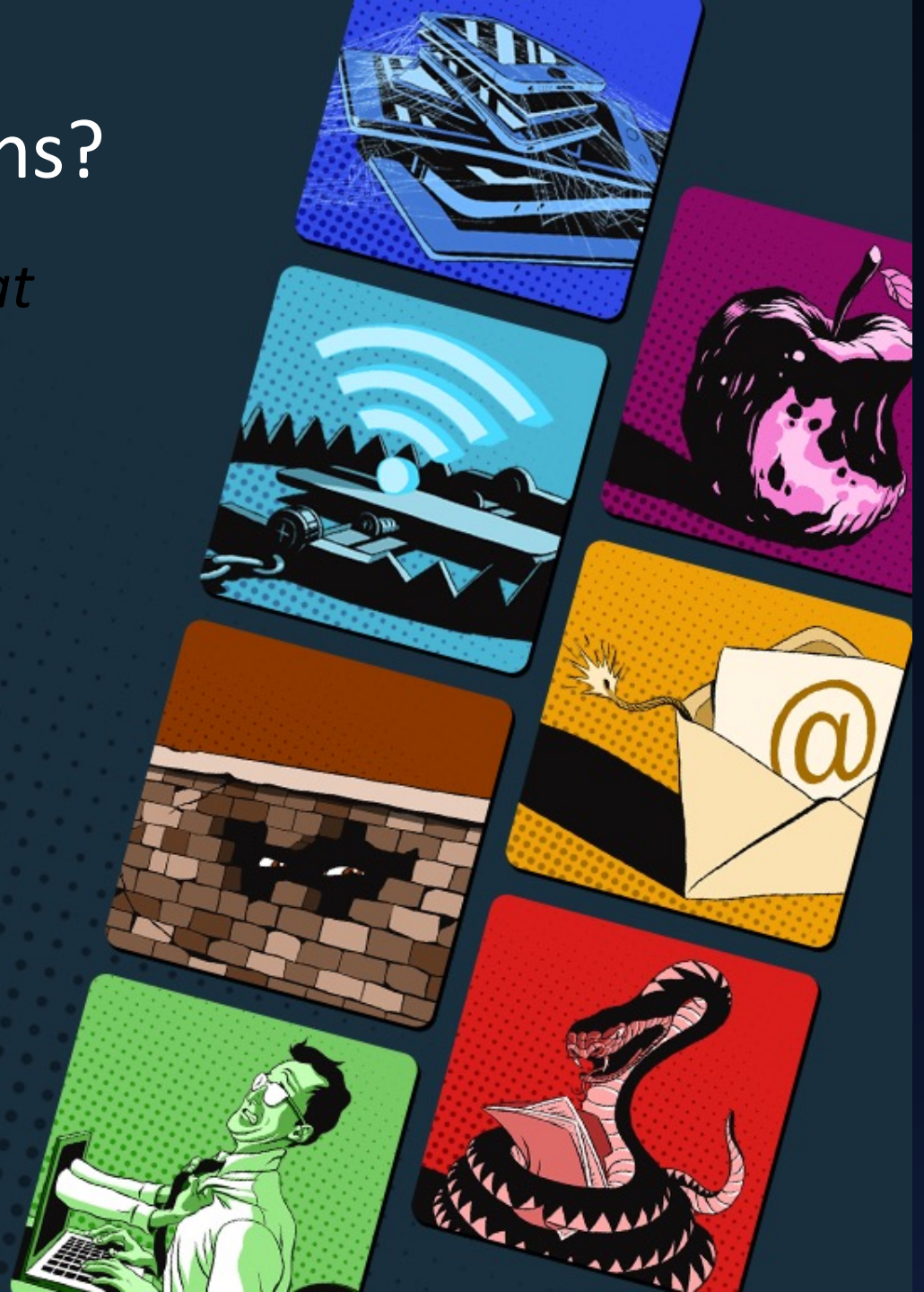
Know them. Fear them. Fix them.



What are Deadly IT Sins?

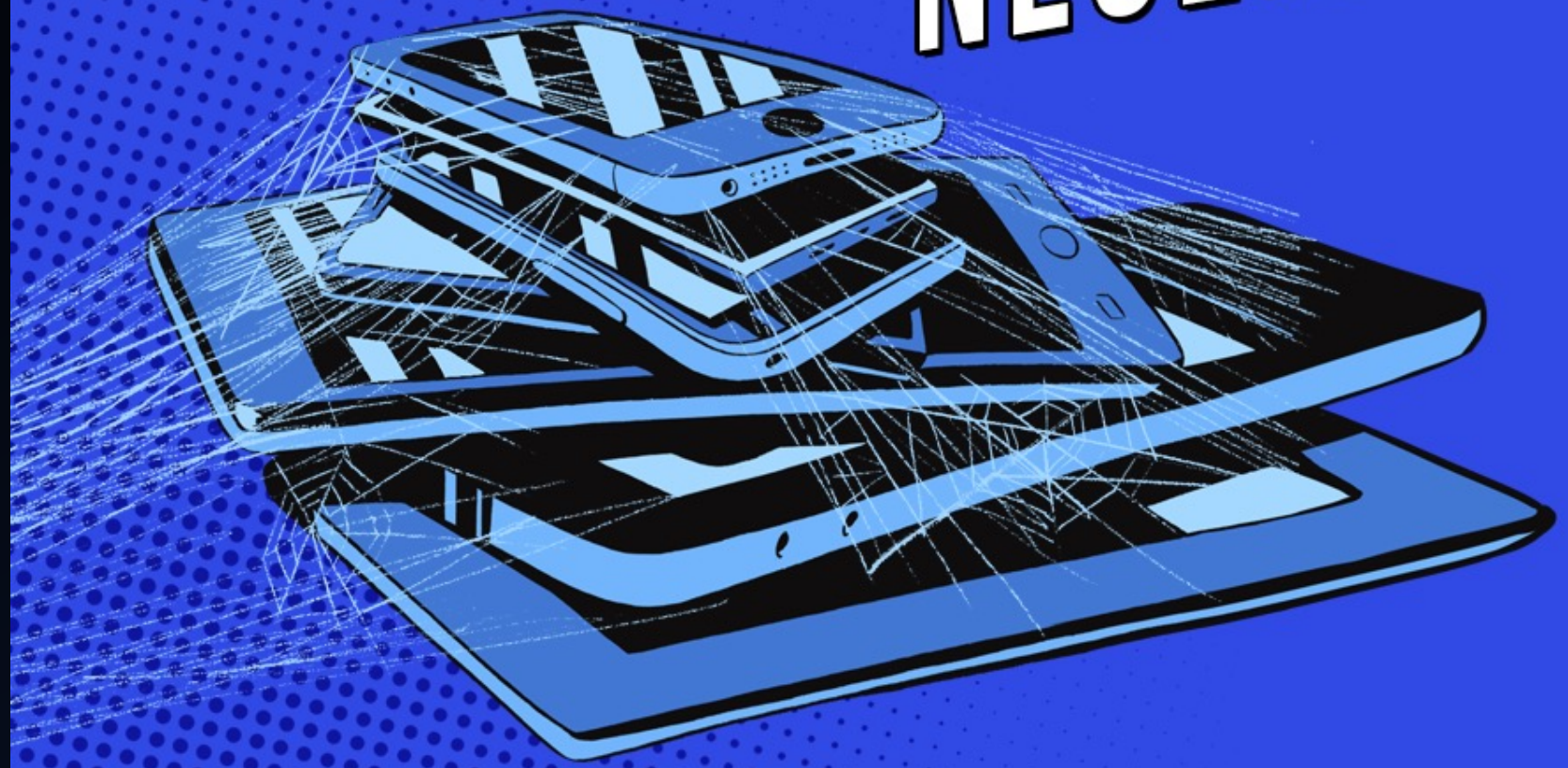
Common security pitfalls that are often overlooked…

…putting your network and data at risk!



7 DEADLY I.T. SINS

No.1 MOBILE NEGLIGENCE



Mobile Negligence

7 DEADLY I.T. SINS

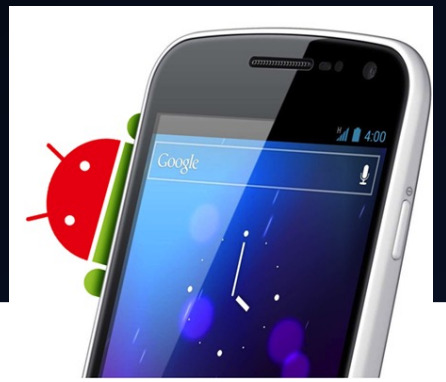
Are you afflicted?



Unsafe practices

64% of users don't lock their phones

+



Malware Growth

Android malware up 1800% in the last 12 months

Data Theft
Financial Consequences
Lost Productivity

Example: NotCompatible.C

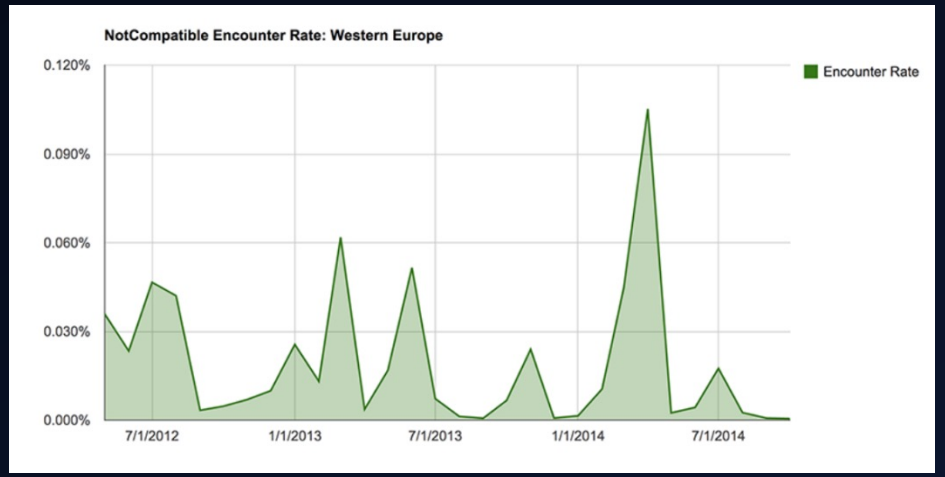
Android Malware

- Establishes a mobile botnet
- Sophisticated, mature, resilient
- Employs encryption and authentication with C&C servers
- Distributed through spam and hijacked websites – uses social engineering



Can be very dangerous in a corporate environment

- Device's network can be relayed to C&C to identify the organization
- Infected phones can provide a proxy to other systems on the network



7 DEADLY I.T. SINS

The path to absolution

Make sure you can **manage** and **secure** your **mobile devices** and your **corporate network**

Mobile Device Management:

- Enforce strong passwords
- Control unwanted/unknown apps
- Block Android malware

Mobile Network Protection:

- Next-generation Firewall
- Mobile Network Access Control
- Advanced Threat Protection



7 DEADLY I.T. SINS



MAC MALICE

No.2

Mac Malice

7 DEADLY I.T. SINS

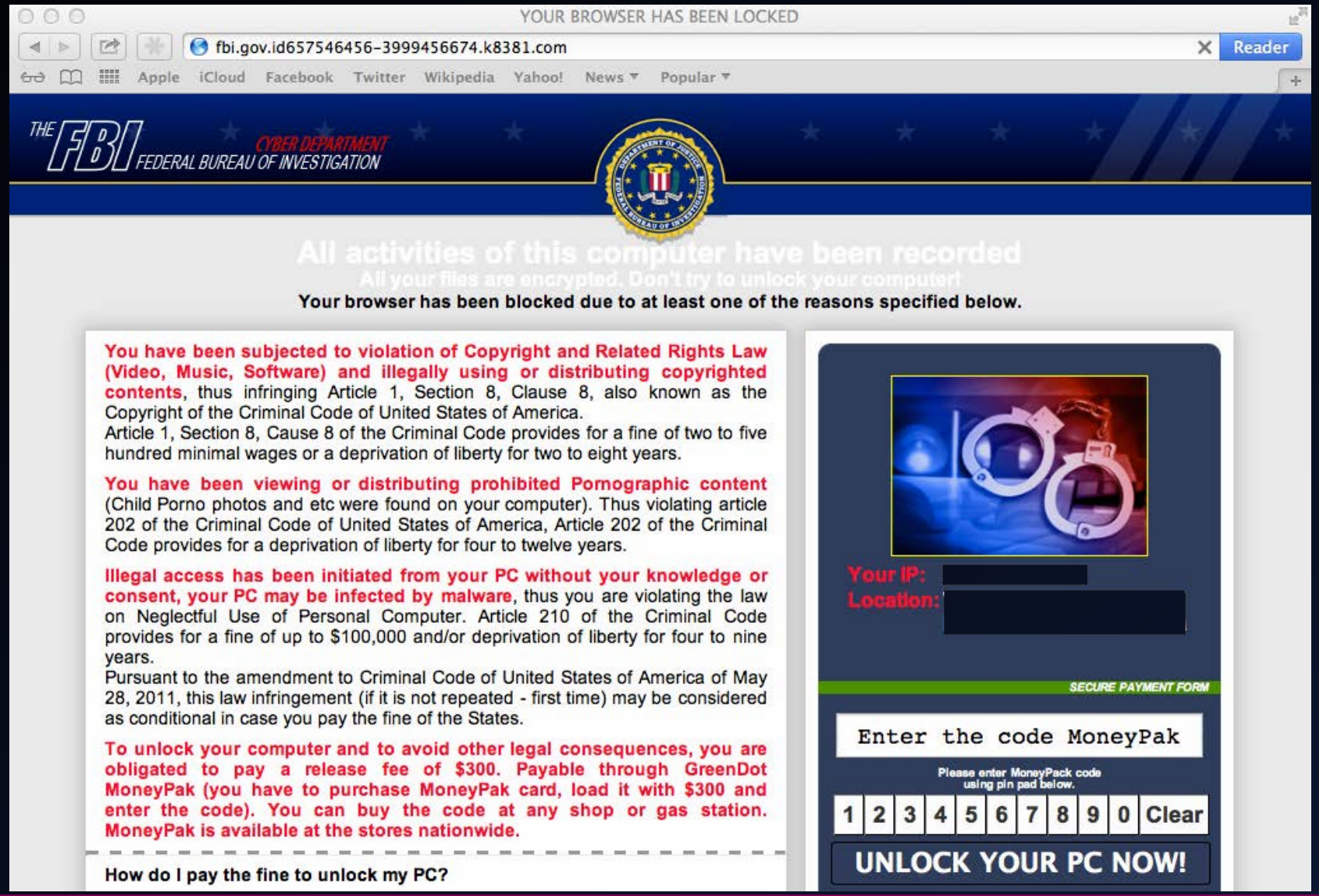
Macs are common in corporate environments and attackers are increasingly targeting them.

- Macs are an easy target because they often lack endpoint protection
- Malware signed with a working Apple Developer ID is on the rise
- Macs can host and spread Windows malware



Don’t let Macs be the chink in your security armour!

Example: Mac Ransomware



Turn that malice into loving care

7 DEADLY I.T. SINS

1. Keep unsigned applications off your Macs
2. Ensure your Macs are secured with business-grade endpoint protection
3. Provide your Macs the same loving policies you provide your Windows systems

Common security loophole

Web control policies for PC users are enforced on their Windows machines.

But if the policy doesn’t extend to Macs, they become the weak link in your security.

7 DEADLY I.T. SINS

UNSECURE WI-FI

No.3



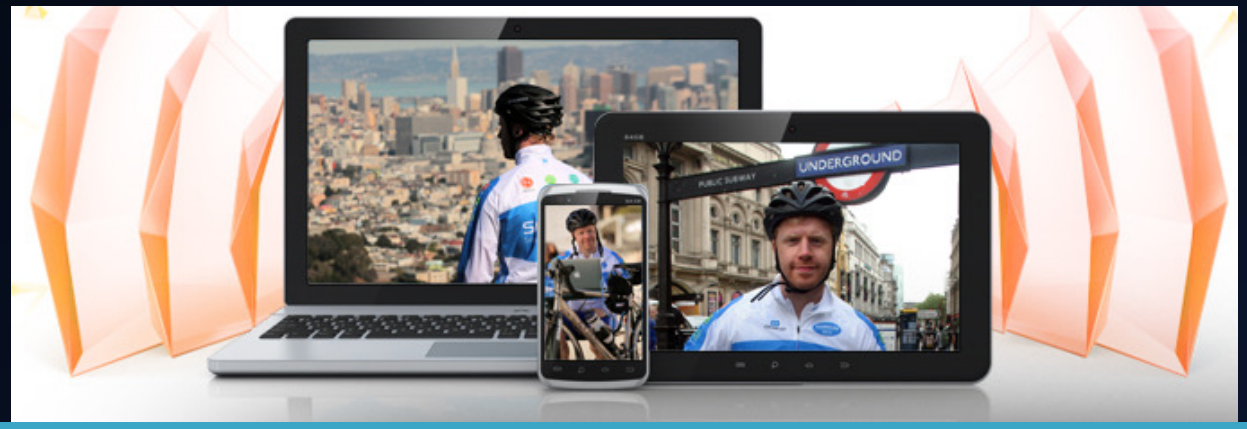
Unsecure Wi-Fi

7 DEADLY I.T. SINS

Project Warbike, London:

- 107,000 wireless networks surveyed
- 27% had poor or no security
- Highest density in streets with high numbers of small business

Unsecure Wi-Fi puts your network and your data at risk



Examples: Wi-Fi Attacks

- Passive Attacks
  - Eavesdropping… Snooping data
  - Impossible to detect… Steal email contents

- Active Attacks
  - Access the network
  - Setup Man in the Middle
  - Snoop Traffic
  - Redirect Users
  - Authenticate to servers
  - Steal Data
  - Denial of Service



Be a Saint not a Sinner

7 DEADLY I.T. SINS

Make sure your Wi-Fi network – and the data on it – is secure.

- ❑ Use business grade Wi-Fi access points
- ❑ Enforce standard network security policies
- ❑ Scan all network traffic
- ❑ Block access for insecure mobile devices
- ❑ Provide connection profiles for your users
- ❑ Keep guest networks separate
- ❑ Keep it simple

Forrester 5 S's

- Scalable
- Shared
- Simplified
- Standardized
- Secure

The Forrester Wave: Wireless Local Area Network Solutions, Q3 2014, Forrester Research, Inc., August 29, 2014.

7 DEADLY I.T. SINS

UNENCRYPTED EMAIL

No.4



Unencrypted Email

144.8 billion emails sent every day

Snooping



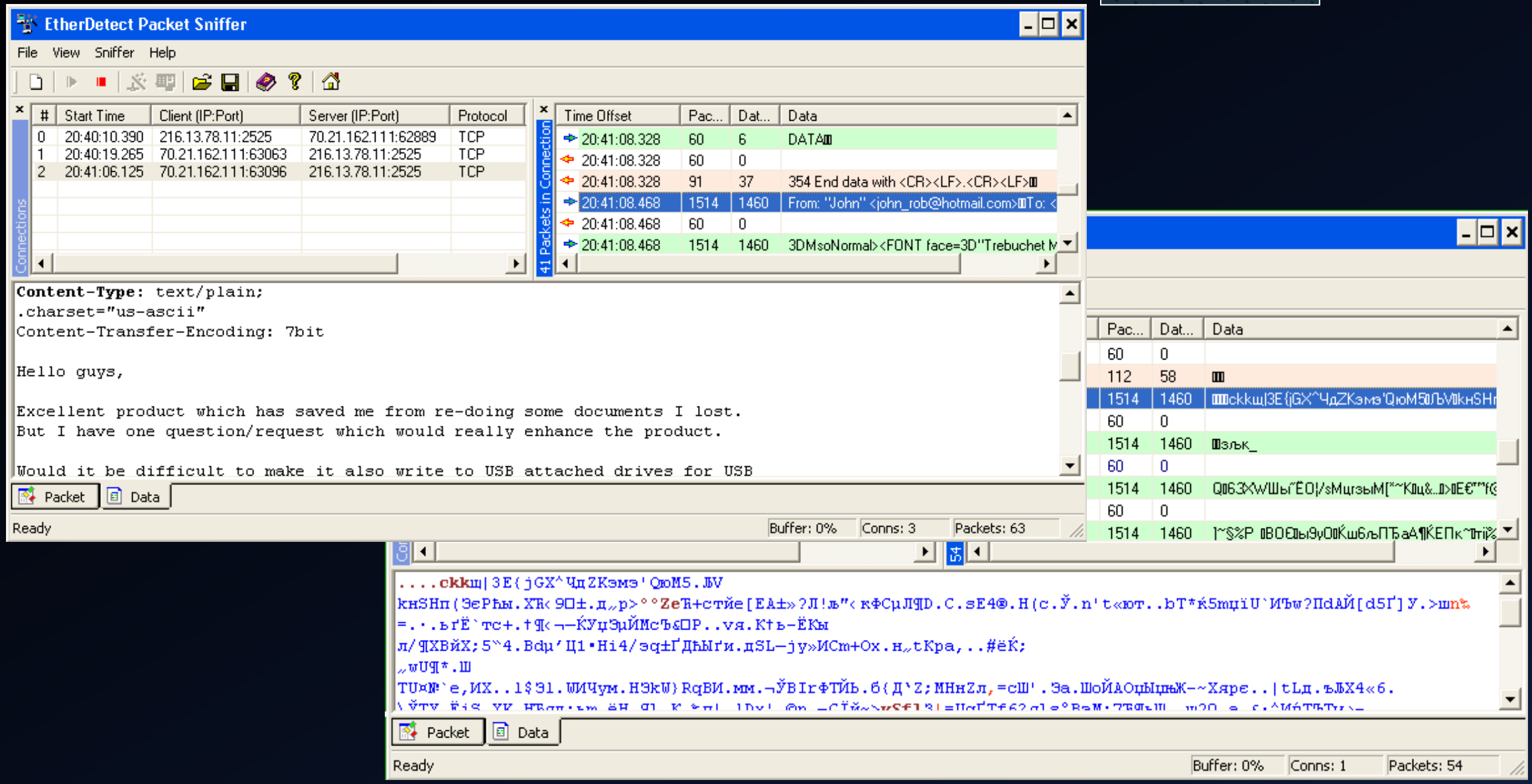
Data loss





Example: Snooping Mail is Trivial

7 DEADLY I.T. SINS



Stop procrastinating – liberate yourself

Your checklist for Email Security:

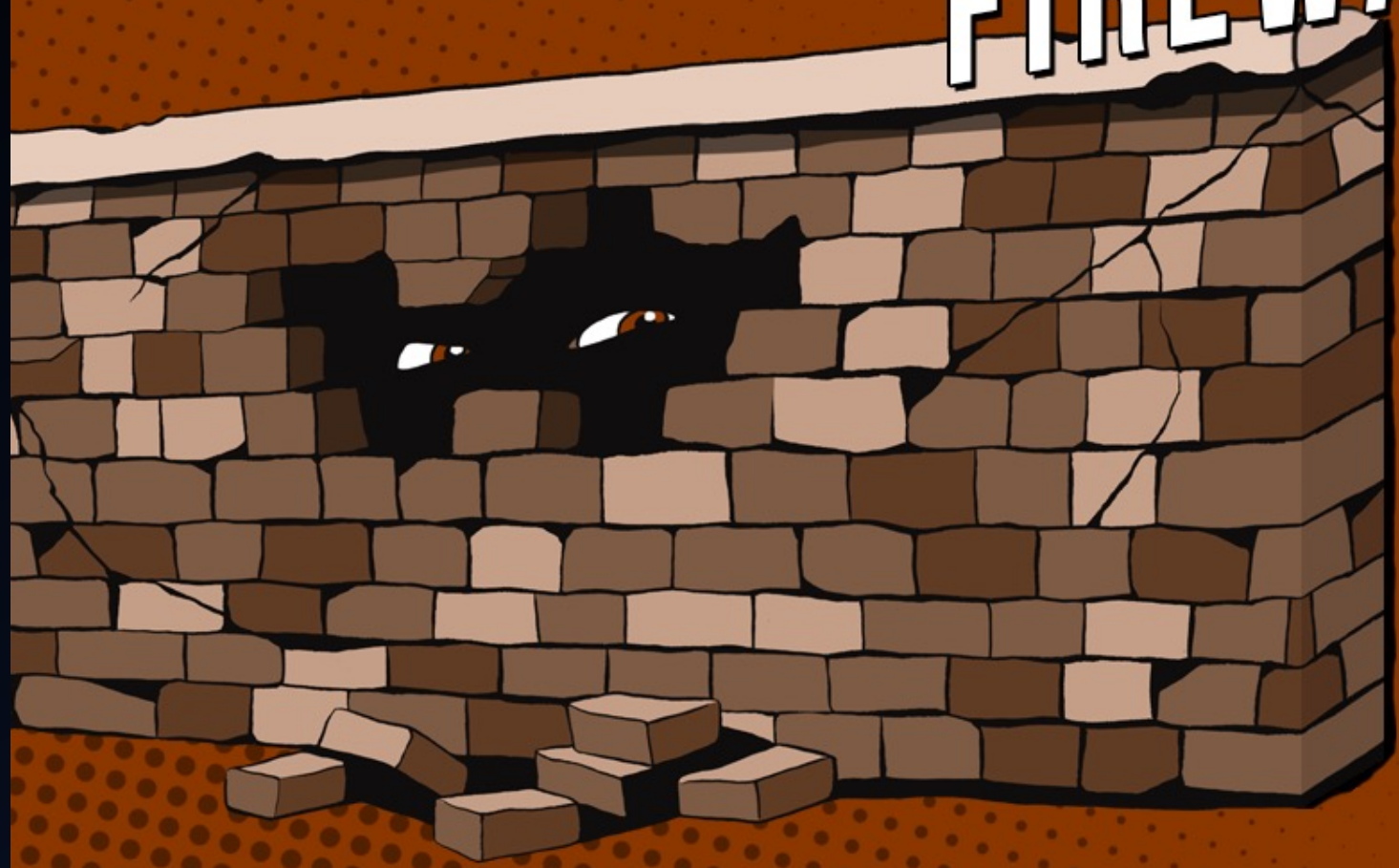
- ❑ Implement a policy
- ❑ Educate Users
- ❑ Implement Email Encryption that..
  - Integrates DLP, encryption and anti-spam
  - Easy to deploy
  - Detects sensitive data automatically
  - Users will love to use – no changes for them
  - Keeps you informed

Email Encryption & DLP can be…

- Simple
- Elegant
- Effective
- Affordable
- Usable

7 DEADLY I.T. SINS

No.5 FAULTY FIREWALL



What makes a Faulty Firewall?

7 DEADLY I.T. SINS

Bandwidth demands

Social Media

Advanced threats

Poor performance

Management complexity

Missing functionality

Limited visibility



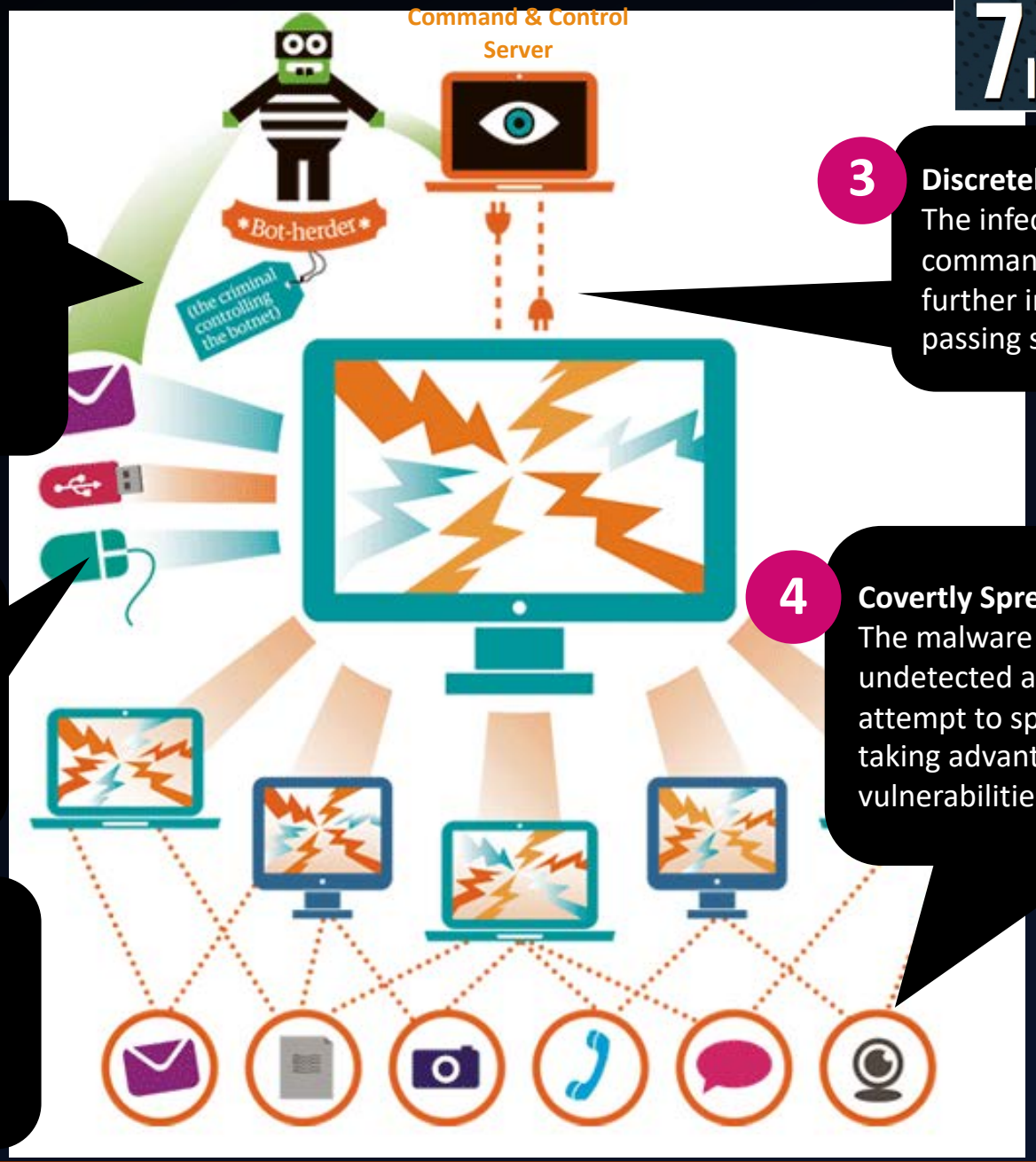
Example: Advanced Threats

7 DEADLY I.T. SINS

1 Targeted Attacks
Advanced Persistent Threats (APTs) are usually targeted at specific industries or organizations, but even small businesses can be targeted as well.

2 Entry Point
Targeted or not, the initial system is usually infected by either:
- Visiting an infected website
- Opening an email attachment
- Plugging-in a USB stick

5 Silently Exfiltrate Data
The malware may attempt to steal information from emails, documents, Skype or IM conversations, or even webcams depending on it's intentions



3 Discretely Call Home
The infected system connects to the command & control (C&C) server for further instructions or to start passing sensitive data

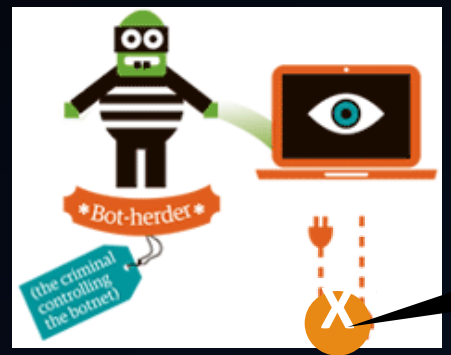
4 Covertly Spread
The malware may choose to remain undetected and move slowly or it may attempt to spread to other systems by taking advantage of unpatched vulnerabilities or using hijacked credentials

What you need

Preventing, Blocking, Identifying, Sandboxing – Made Simple

7 DEADLY I.T. SINS

6 Selective Sandboxing
Suspicious samples representing potential unknown threats are sent to a sandbox for analysis. New threat intelligence is passed back to the Firewall.



3 Block Network Attacks
Next-gen firewall and IPS block network attacks and prevent breaches at the network gateway

Sandbox

1 Multi-layered Protection
Integrated web, email and endpoint protection prevent infections from entering the network in the first place

4 Block Calls-Home
Look across a variety of network traffic vectors to identify C&C traffic patterns and block them

2 Web Malware Detection
Advanced web malware detection that can emulate JavaScript to catch even the most sophisticated obfuscated and polymorphic threats

5 Identify Infected Systems
Report and alert on infected hosts attempting to communicate with C&C and contain them.

7 DEADLY I.T. SINS

Redemption is here

Your checklist for a new firewall:

1. ❑ Usability
2. ❑ Performance in real-life scenarios
3. ❑ Advanced Protection capabilities
4. ❑ Security expertise
5. ❑ Reporting

7 DEADLY I.T. SINS



UNENCRYPTED FILES

No.6

7 DEADLY I.T. SINS

Unencrypted Files



Example: Sinfully Unencrypted Laptops

7 DEADLY I.T. SINS

Laptop stolen with health information of 620,000 Albertans

Health officials recently informed of theft from last September

CBC News Posted: Jan 22, 2014 3:30 PM MT | Last Updated: Jan 23, 2014 6:43 PM MT



Stay Connected with CBC News

Mobile Facebook Podcasts Twitter Alerts Newsletter

Latest Edmonton News Headlines



- Edmonton police learned about alleged ISIS recruiter from CBC story
- Plunge in oil price seen as opportunity for Alberta

Albe

Stolen Laptops, Hard Drives Expose Over 100,000 People's Personal Data

The data potentially exposed includes names, addresses, phone numbers and Social Security numbers.

By **Jeff Goldman** | Posted February 25, 2015

Share



Several thefts of unencrypted laptops and hard drives recently exposed a significant number of people's personal information.

The Boston Baskin Cancer Foundation recently acknowledged that 56,694 patients' and employees' personal information may have been exposed when an unencrypted external hard drive was stolen from an employee's home on December 2, 2014 (h/t DataBreaches.net).

The drive contained patient demographic information, birthdates, Social Security numbers, phone numbers and first and last dates of clinic visits for patients seen between 2008 and July 2014. For employees, the drive held titles, office locations, Social Security numbers, birthdates, pay rates, and dates of employment.

Coca-Cola Says 74,000 Affected After Company Laptops Stolen



Coca-Cola's shares fell 1 percent to $38.84 at the close in New York and added 14 percent last year. Photographer: Dario Pignatelli/Bloomberg

Redemption the easy way

7 DEADLY I.T. SINS

Your checklist for encryption:

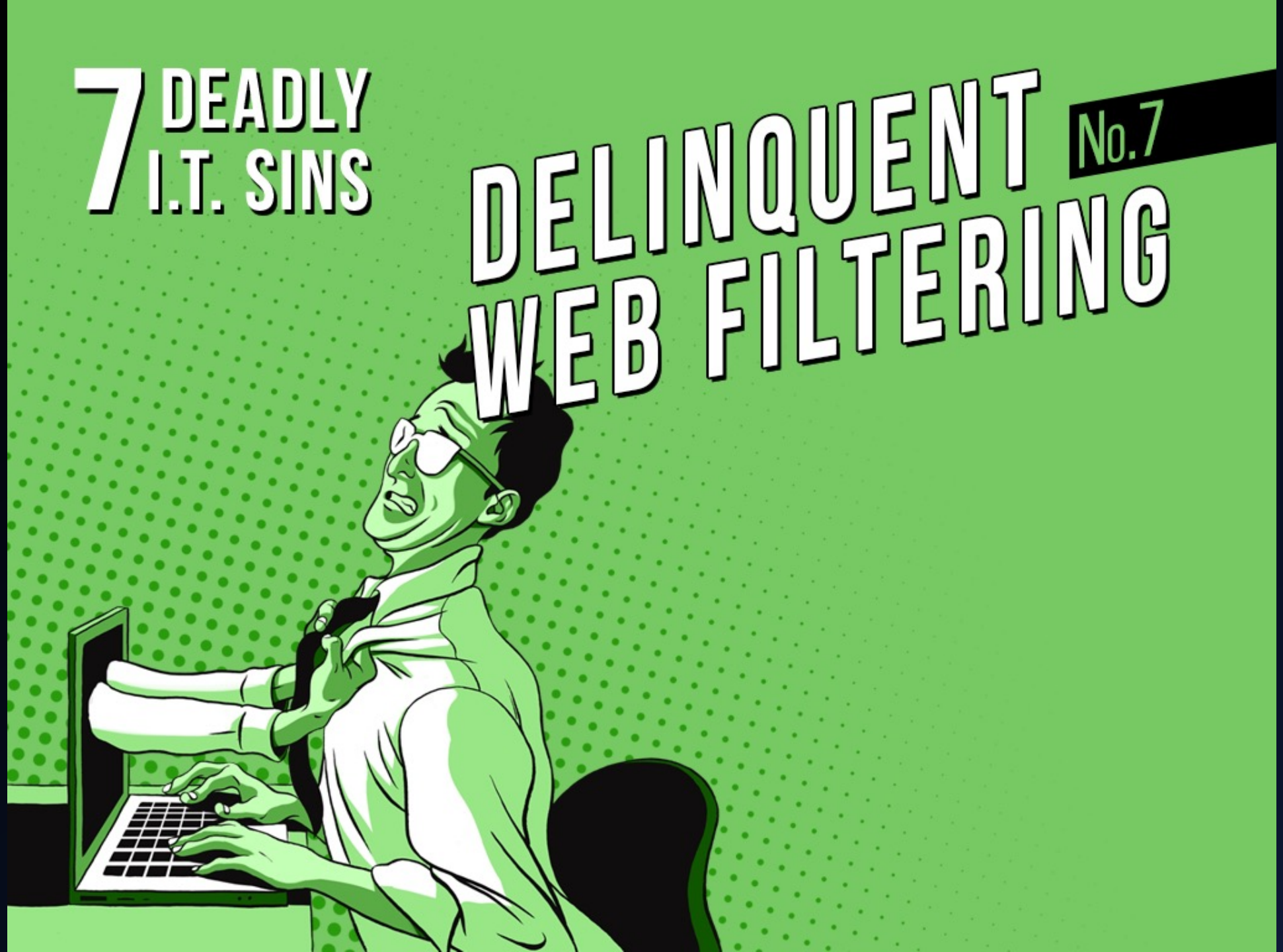
- ❑ Use full-disk encryption on all laptops
- ❑ Use server encryption
- ❑ Encrypt your email (see Sin #4)
- ❑ Implement file encryption across cloud and mobile devices
- ❑ Reporting, Management, Auditing



7 DEADLY I.T. SINS

No.7

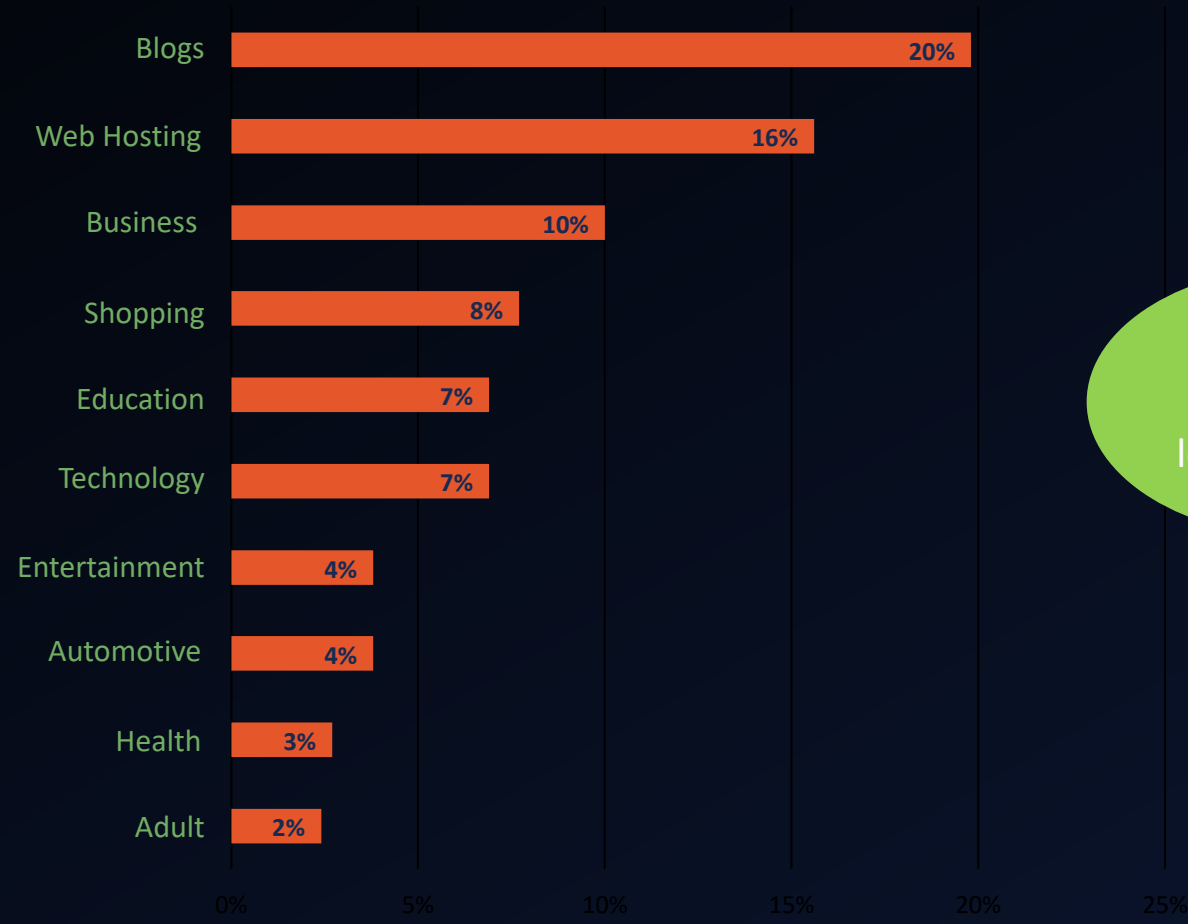
DELINQUENT WEB FILTERING



Delinquent Web Filtering

7 DEADLY I.T. SINS

Top 10 infected web site categories



40,000
New web threats every day

80%
Malware on legitimate sites

$400M
Stolen through GameOver malware

Example Web Attack

7 DEADLY I.T. SINS

Entry Point

Drive-by-download from a hijacked website or an email with a malicious link

Distribution

Initial malware redirects based on what it's working with (Windows/Mac, IE/Safari, Java)

Exploit

Exploit pack attempts to leverage a number of vulnerabilities

Infection

Download of a malicious payload

Execution

Malware calls home with sensitive data

TMZ.com

The New York Times

Spotify

London Stock Exchange



ЭКСПЛОИТЫ	ЗАГРУЗКИ	% ↑
Java Rhino	1985	96.88
MDAC	28	1.37
PDF ALL	12	0.59
PDF LIBTIFF	10	0.49
HCP	9	0.44
Java OBE	5	0.24



Recap

7 DEADLY I.T. SINS

- ❑ Mobile Negligence
- ❑ Mac Malice
- ❑ Unsecure Wi-Fi
- ❑ Unencrypted E-mail
- ❑ Faulty Firewall
- ❑ Unencrypted Files
- ❑ Delinquent Web Filtering

And yes, there are more IT Sins than those we've listed here.