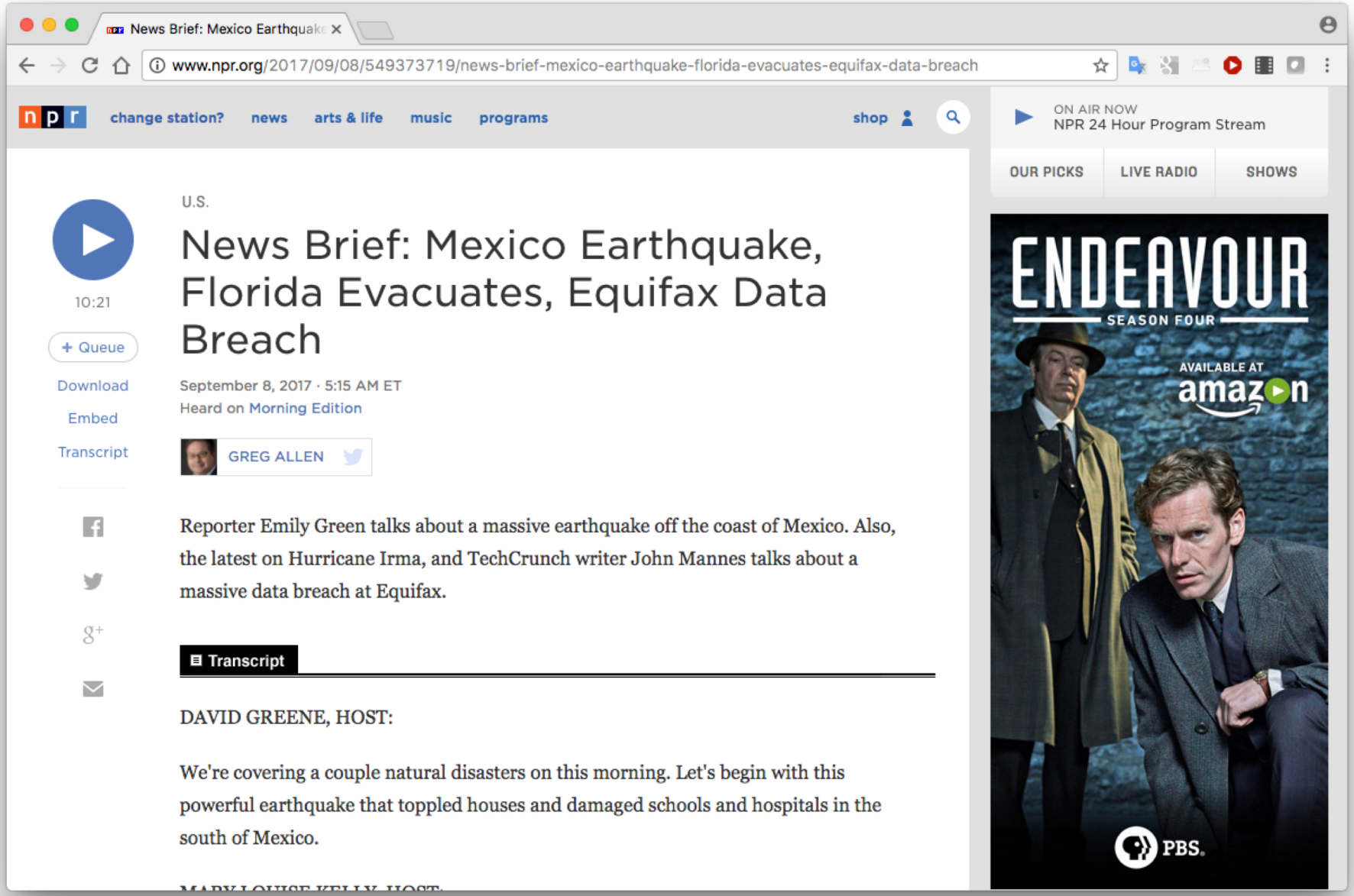
EWD - Security part

Setting the scene

Security part of module: main topics

- Introduction
  - Threats, attacks, vulnerabilities; Security services
- Cryptography
  - Symmetric encryption
  - Public key cryptography
  - Authentication and integrity
  - Key management and certificates
- Web application threats and vulnerabilities
  - Common vulnerabilities
  - Penetration testing
  - Threat modelling
- Web application protection
  - Input validation
  - Web authentication schemes
  - Secure key and password storage

Security news stories…



Security news stories…

https://komonews.com/news/local/personal-data-of-nearly-1-million-uw-medicine-patients-exposed-online

KOMONEWS NEWS WEATHER SPORTS REFINED CHIME IN WATCH

Personal data of nearly 1 million UW Medicine patients exposed online

by Tammy Mutasa | KOMO News | Wednesday, February 20th 2019

Security news stories…

Microsoft spots Russian hackin

https://news.sky.com/story/microsoft-spots-russian-hacking-campaign-ahead-of-eu-elections-11642702

sky news

Watch Live

Home UK World Politics US Ocean Rescue Science & Tech Business Ents & Arts Offbeat More

Microsoft spots Russian hacking campaign ahead of EU elections

According to Microsoft, the campaign is using the same tools which were used in an attempt to influence the US election in 2016.

By Alexander J Martin, technology reporter

Wednesday 20 February 2019 11:56, UK

EUROPEAN UNION MICROSOFT RUSSIA

Security news stories…

'Third Party Data Breaches' Le

https://extra.ie/2019/01/11/business/irish/bank-of-ireland-restricts-fraud-fears

Extra.ie Read more about it

Home News Sport Business Entertainment

‘THIRD PARTY DATA BREACHES’ LEAD BANK OF IRELAND TO RESTRICT DEBIT CARDS

By **George Morahan** - 11/01/2019

Bank of Ireland has restricted the use of some customers’ debit cards amid ongoing concerns about fraud.

Affected customers will be prevented from using their cards for online and contactless transactions until they receive their new cards, which have been issued as a precaution.

The bank’s decision stems from what it said was an ‘increase in third party data breaches’, citing breaches at Ticketmaster and the Marriott Hotel Group.

MORE BUSINESS

Security news stories…

Ireland's Privacy Watchdog Pro

Information Security Media Group, Corp. [US] | https://www.bankinfosecurity.com/irelands-privacy-watchd...

Topics News Training Resources Events Jobs

TRENDING: Webinar | Beyond Managed Security Services: SOC-as-a-Service for Financial Institutions •

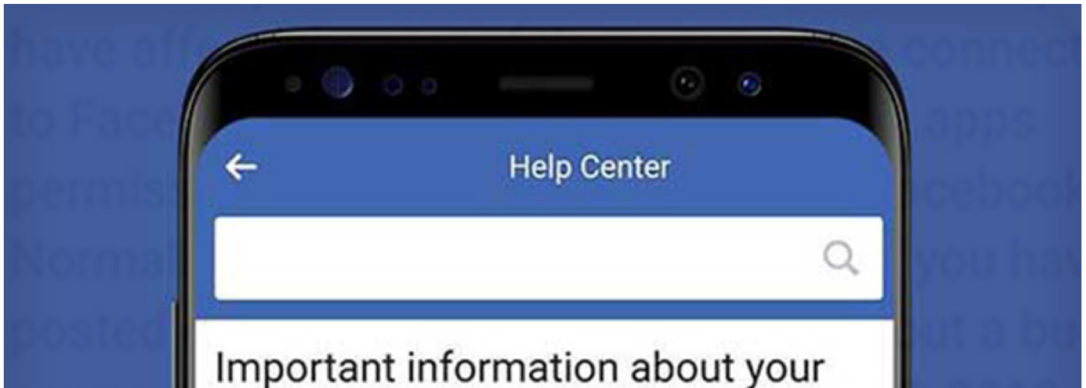
Breach Notification , Data Breach , General Data Protection Regulation (GDPR)

Ireland's Privacy Watchdog Probes Facebook Data Breaches

6.8 Million Users' Private Photos Exposed, Triggering GDPR Investigation

Mathew J. Schwartz (euroinfosec) • December 17, 2018 2 Comments

Twitter Facebook LinkedIn Credit Eligible Get Permission



GET DAILY EMAIL UPDATES

Covering topics in risk management, compliance, fraud, and information security.

Email address Submit

By submitting this form you agree to our Privacy & GDPR Statement

Security news stories…

Yahoo's 2013 Data Breach Affected Three Billion Accounts

Posted on October 4, 2017 by Alex Perala

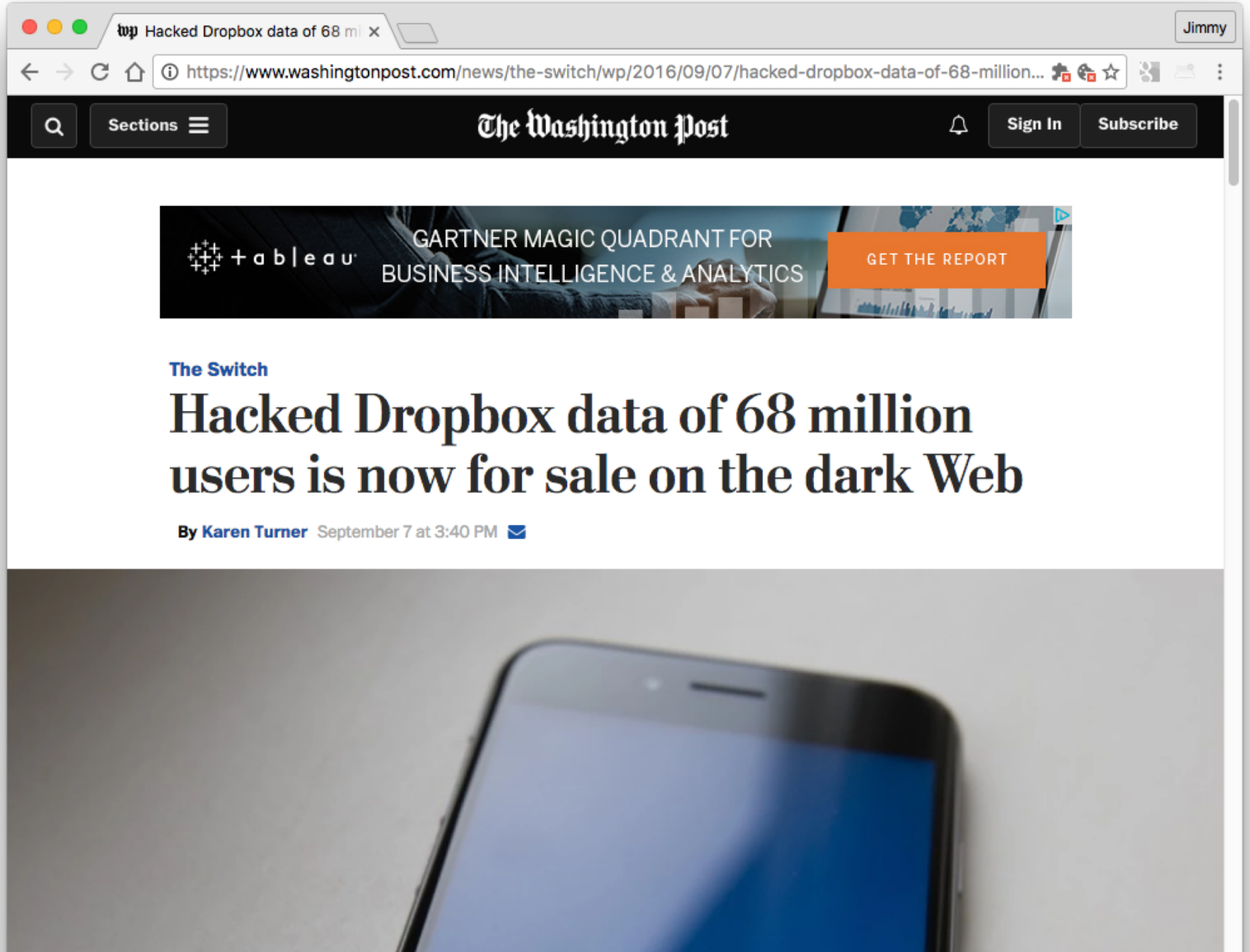
> **"There are a couple of silver linings here. One is that it can't get any worse, since the three billion compromised accounts represent Yahoo's entire account database."**

Yahoo's 2013 data breach affected three billion accounts, the company has now revealed.

It is yet another upsizing of the damage on Yahoo's part, with the company initially having announced that the credentials of 200 million users had appeared for sale online, and later admitting that half a billion accounts had been compromised. Its latest revelation is the result, the company says, of collaboration with independent forensic investigators.

There are a couple of silver linings here. One is that it can't get any worse, since the three billion compromised accounts represent Yahoo's entire account database. The other is that

Security news stories…



Security news stories…

WannaCry attacks prompt Mic

Secure | https://www.theguardian.com/technology/2017/jun/14/wannacry-attacks-prompt-microsoft-to-release-updates-for...

Windows

WannaCry attacks prompt Microsoft to release Windows updates for older versions

The company typically releases security updates for operating systems it still supports - but in wake of serious cyber-attack it has reassessed the policy

This article is 2 months old

267

Alex Hern

@alexhern

Wednesday 14 June 2017 12.26 BST

Security news stories…

Just One Photo Can Silently Ha

Jimmy

www.forbes.com/sites/thomasbrewster/2016/09/06/google-android-one-photo-hack/#15ab50961555

Forbes / Security / #CyberSecurity

SEP 6, 2016 @ 03:47 PM 10,503 VIEWS

The Little Black Book of Billionaire Secrets

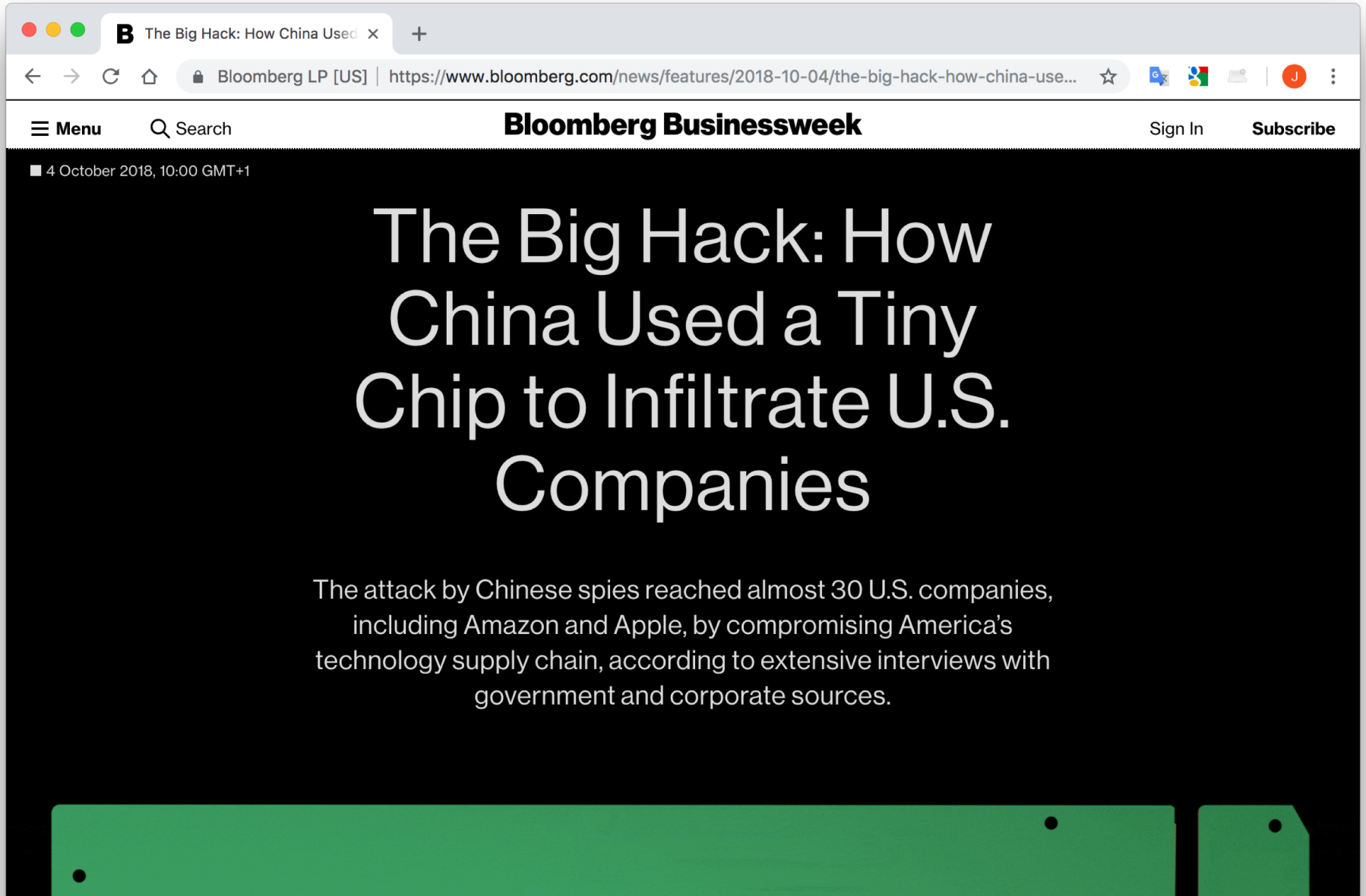
Just One Photo Can Silently Hack Millions Of Androids

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

SHARE

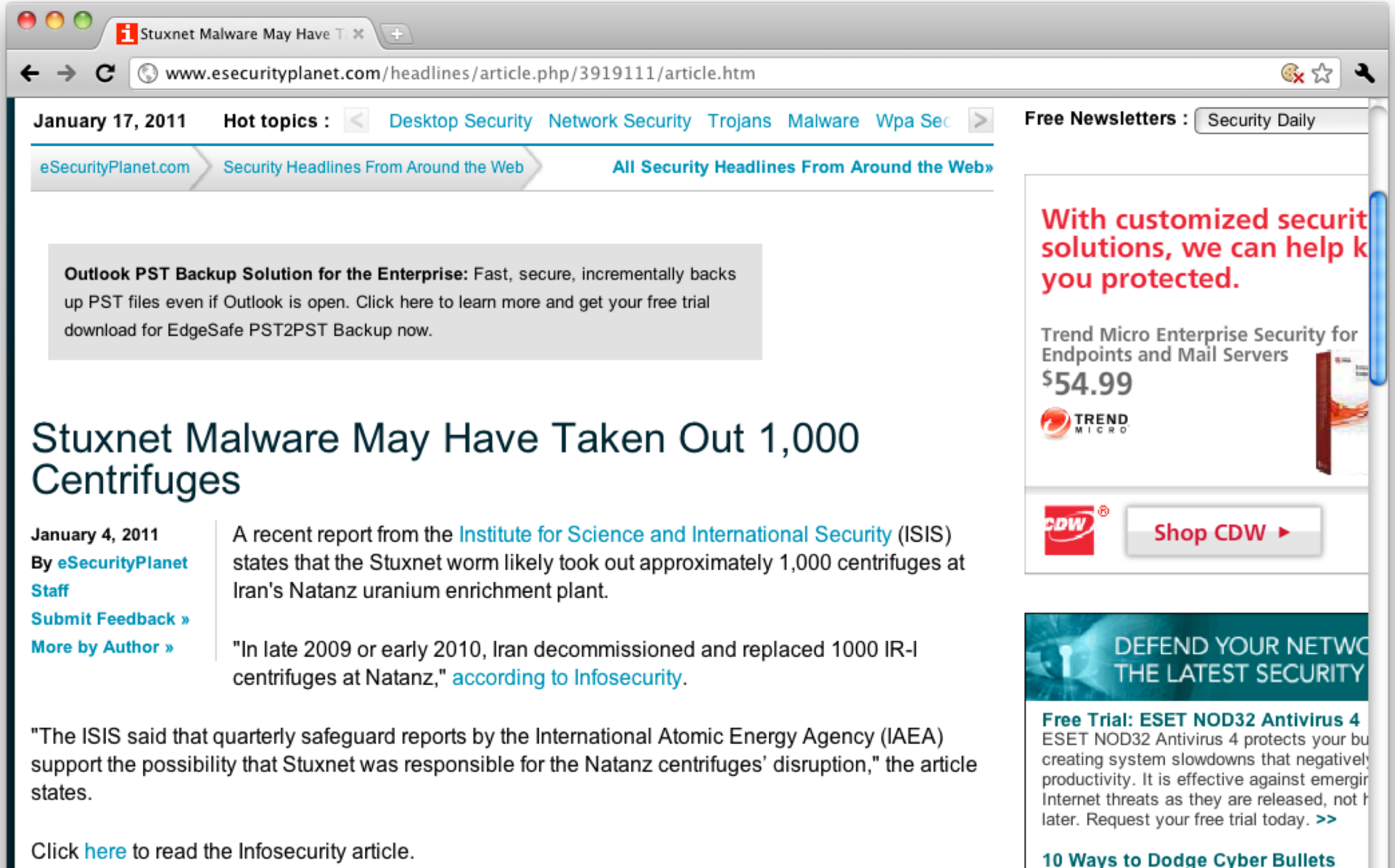
Security news stories…

Security news stories…

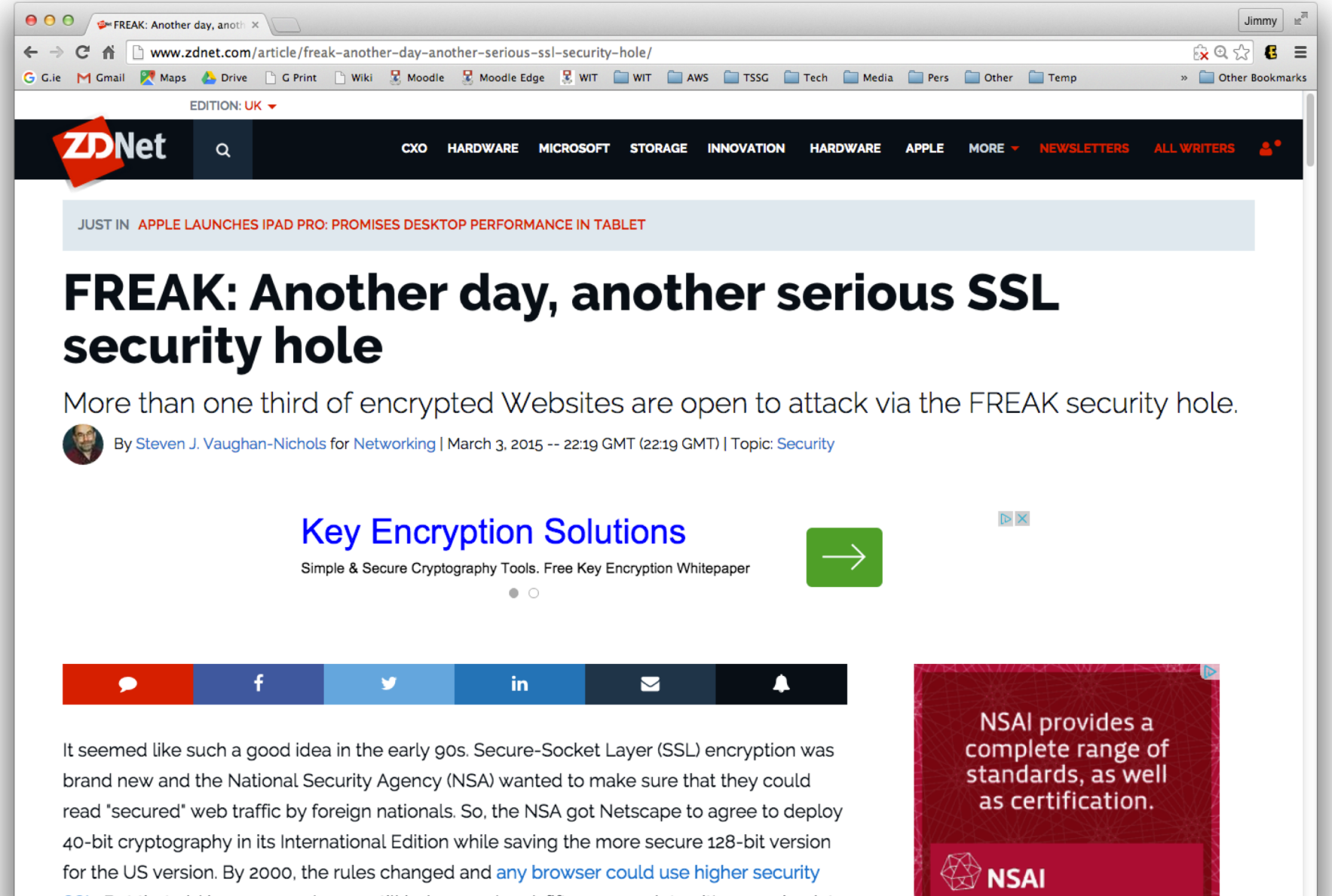


Security news stories…

Security news stories…



Security news stories…



Security news stories…

Extremely critical crypto fl ×

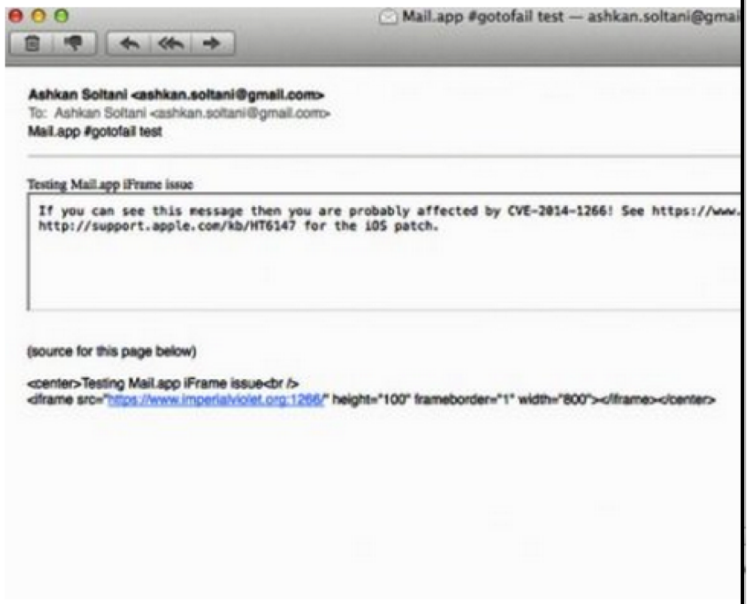
arstechnica.com/security/2014/02/extremely-critical-crypto-flaw-in-ios-may-also-affect-fully-patched-macs/

MAIN MENU ▾ MY STORIES: 25 ▾ FORUMS SUBSCRIBE JOBS

Extremely critical crypto flaw in iOS may also affect fully patched Macs

Coding blunder that exposed sensitive data may still be

by **Dan Goodin** - Feb 22 2014, 7:45pm GMT



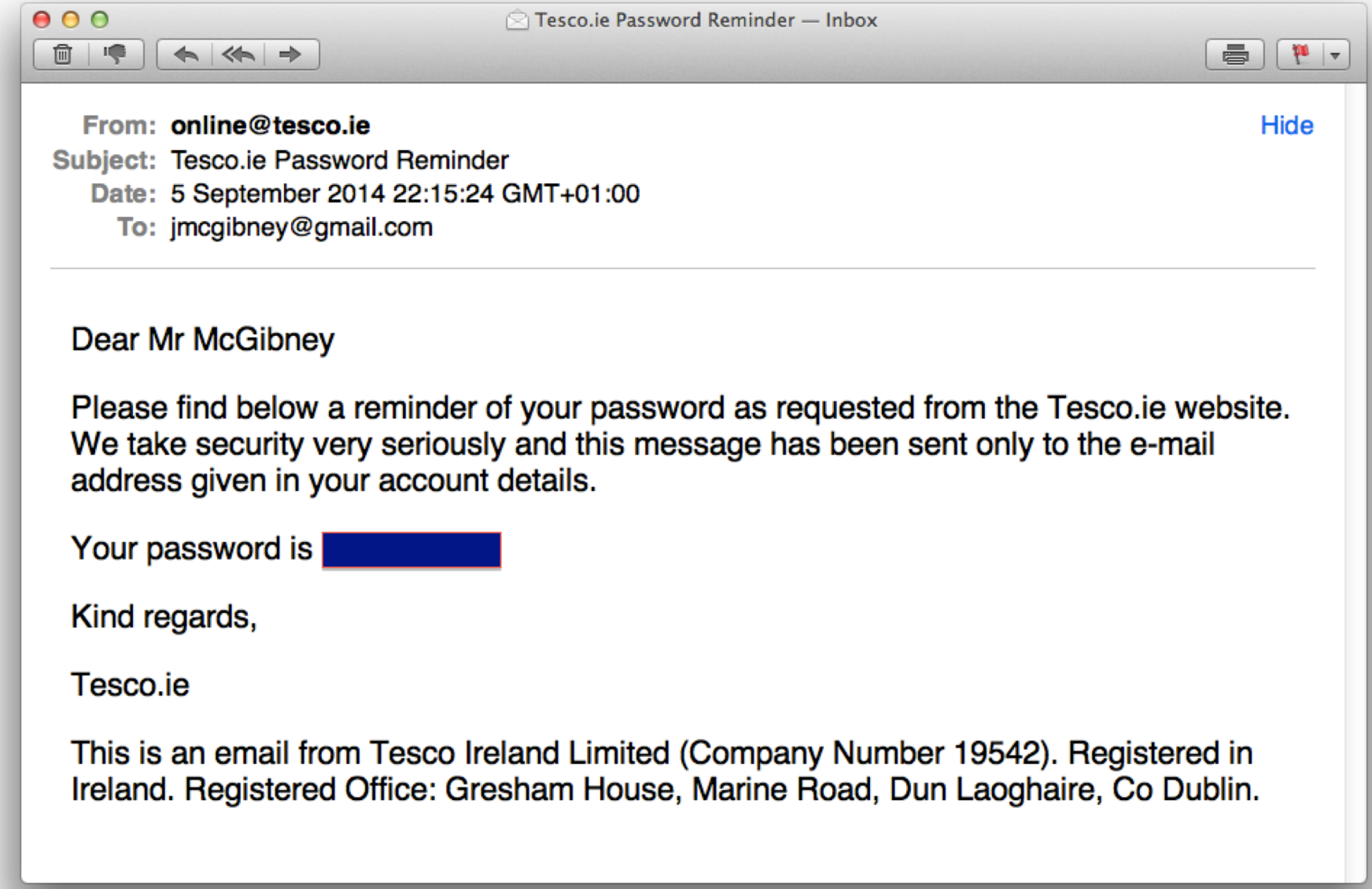
Ashkan Soltani

A critical iOS vulnerability that Apple patched on Friday gives a

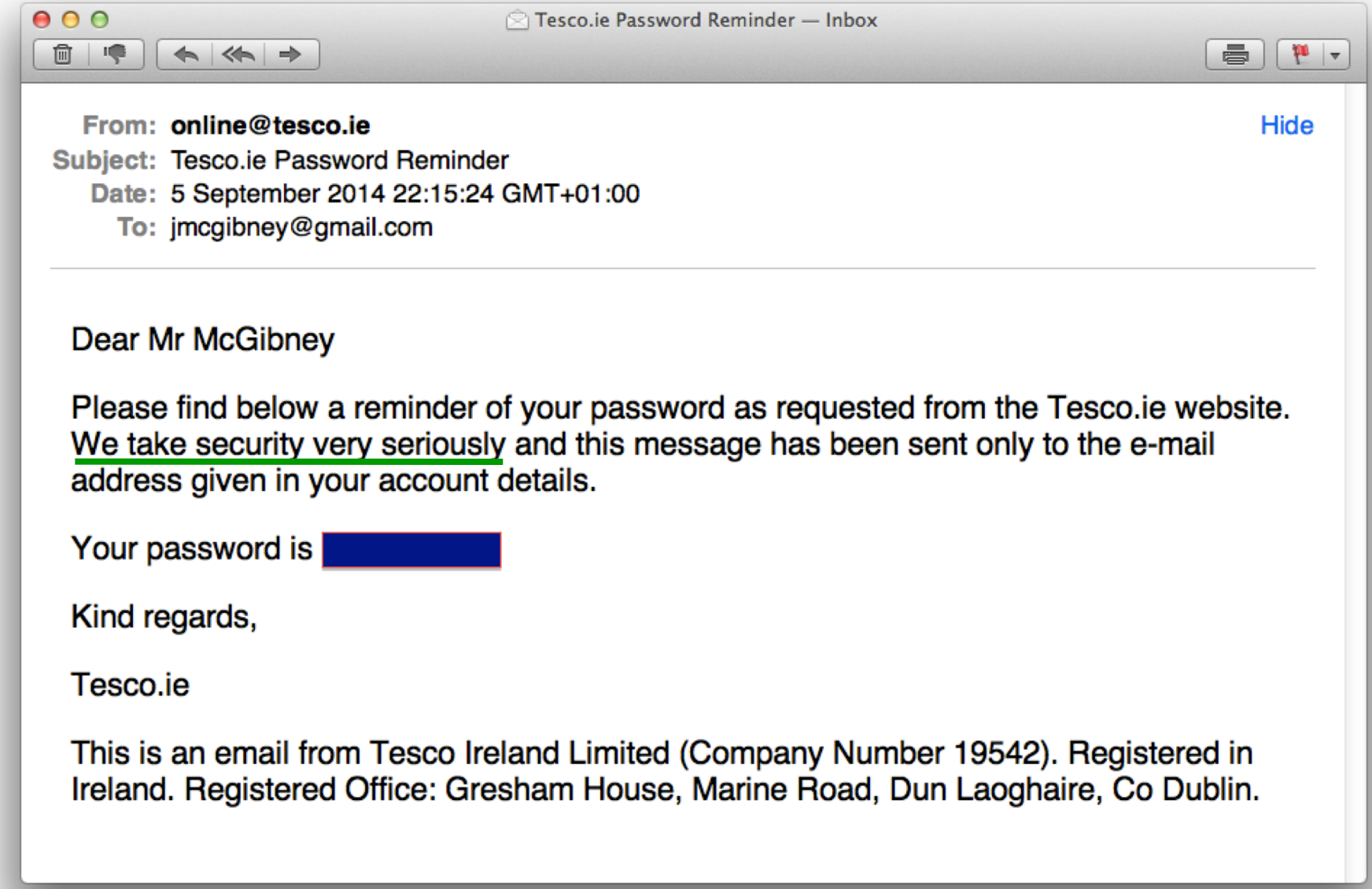
Stick a Tile to anyth
track it v

```
    hashOut.length = SSL_SHA1_DIGEST_LEN;
    if ((err = SSLFreeBuffer(&hashCtx)) != 0)
        goto fail;

    if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;

        err = sslRawVerify(ctx,
                           ctx->peerPubKey,
                           dataToSign,                /* plaintex
                           dataToSignLen,             /* plaintext length
                           signature,
                           signatureLen);
        if(err) {
                sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify
                    "returned %d\n", (int)err);
                goto fail;
        }

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
```

Anything wrong with this?



Anything wrong with this?



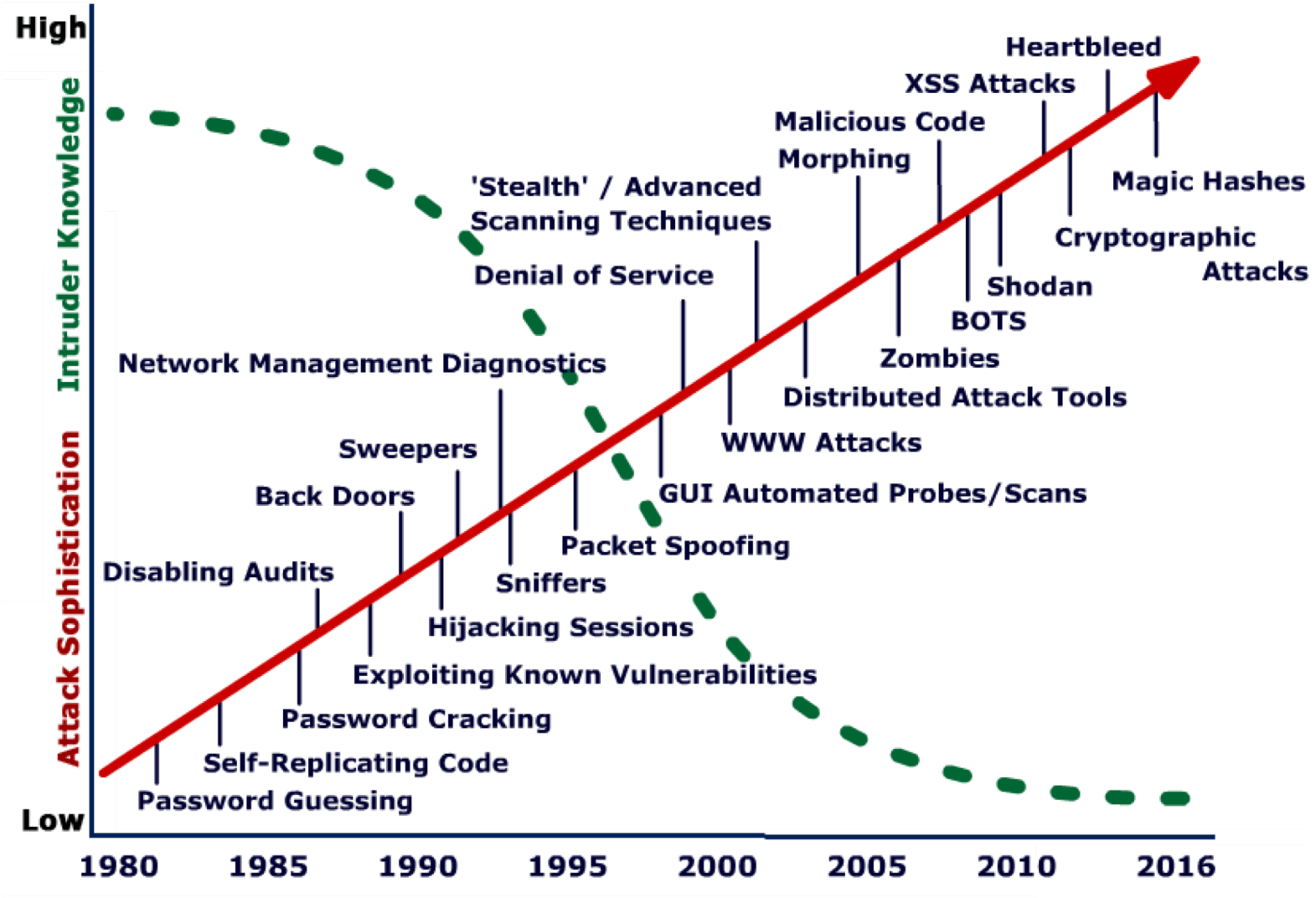
Security in context

- Increasing reliance on IT & networks for just about everything:
  - Communications (phone, email, social networks)
  - Finance
  - Supply chain (e.g. food on supermarket shelves)
  - Electricity generation & distribution
  - Industrial control systems
  - Water supply
  - Transportation
- How long could we cope without these?

SecurityFocus.com – new vulnerabilities snapshot

19-02-2019	LibVNCServer Incomplete Fix Multiple Heap **Buffer Overflow** Vulnerabilities
19-02-2019	Elasticsearch Logstash CVE-2019-7612 Information Disclosure Vulnerability
19-02-2019	WordPress CVE-2019-8943 Directory Traversal Vulnerability
19-02-2019	WordPress CVE-2019-8942 Remote Code Execution Vulnerability
19-02-2019	Horner Automation Cscape CVE-2019-6555 **Arbitrary Code Execution** Vulnerability
19-02-2019	Delta Industrial Automation CNCSoft CVE-2019-6547 **Denial of Service** Vulnerability
20-02-2019	Drupal Core CVE-2019-6340 Arbitrary PHP Code Execution Vulnerability
20-02-2019	Cisco Unity Connection CVE-2019-1685 **Cross Site Scripting** Vulnerability
20-02-2019	Cisco HyperFlex CVE-2019-1667 Arbitrary File Overwrite Vulnerability
20-02-2019	Microsoft Windows HTTP/2 SETTINGS Frames Denial of Service Vulnerability
20-02-2019	Cisco IoT Field Network Director CVE-2019-1698 **XML External Entity** Vulnerability
20-02-2019	Cisco Prime Infrastructure **SSL Certificate Validation Security Bypass** Vulnerability
21-02-2019	Opencontainers runc CVE-2019-5736 Local Command Execution Vulnerability
21-02-2019	WPA2 Key Reinstallation Multiple Security Weaknesses
21-02-2019	Intel Data Center Manager SDK CVE-2019-0110 Information Disclosure Vulnerability
21-02-2019	Intel Data Center Manager SDK Multiple **Privilege Escalation** Vulnerabilities
21-02-2019	Microsoft .NET Framework and Visual Studio CVE-2019-0657 **Spoofing** Vulnerability
21-02-2019	Microsoft Windows Device Guard CVE-2019-0627 Local Security Bypass Vulnerability

Attack Sophistication vs. Intruder Technical Knowledge



Source: CERT Coordination Center, Pittsburgh & Univ of Adelaide (adaptation)

Main Players in Information Security

- Standards Bodies
  - IETF (Internet Engineering Task Force)
    - Internet standards, IPsec, SSL/TLS, …
  - ISO (International Standards Organisation)
    - OSI model; ISO 27000 series of security standards; "Common Criteria" in ISO 15408
  - ITU (International Telecoms Union)
    - Recommendation X.800 on security services
  - NIST (US Nat'l Institute of Standards & Technology)
    - Official US standards (called FIPS); many on security
  - IEEE (Inst of Electrical & Electronics Engineers)
    - Communication standards, most notably IEEE 802 series: Ethernet (802.3), WiFi (802.11), Authentication (802.1x), …
  - Industry domain-specific standards and regulations
    - FDA, PCI DSS, etc

Main Players (continued)

- Government agencies
  - NSA - National Security Agency (US)
    - in the news a lot in recent years
  - Dept of Homeland Security (US)
  - Data Protection authorities (powerful in EU countries)
- The industry
  - Software and equipment vendors, web services
    - Microsoft, Apple, Google, Cisco, Facebook, …
  - Security vendors, outsourcers, consultants
    - Symantec, McAfee, RSA Security, Trend Micro, IBM, HP, …
  - Open source community
    - OpenSSL, Kali Linux, GPG, OWASP, …
  - Certificate authorities
    - VeriSign, DigiCert, Comodo, GeoTrust, GoDaddy, …