Business Cyber Security
Ransomware & Data Breaches

KENNETH ATCHINSON, PE
ASSOCIATE PROFESSOR
BALDWIN WALLACE UNIVERSITY

Speaker Today

- Kenneth Atchinson, PE, is Associate Professor in the Department of Computer Science at Baldwin Wallace University. Currently he is Interim Chair of the department, and heads up the Network and Computer Security Program at BW.
- Kenneth received his Bachelors in Electrical Engineering from Georgia Institute of Technology, and his Masters in Computer Science from Kent State University. He is a Professional Engineers licensed in the State of Ohio
- Before joining faculty at BW, Kenneth worked at a defense contractor in Florida, where he worked as a Software Engineer on several projects, and eventually switched over to Computer System Administration. He has over 8 years of experience as a System Administrator across several companies.
- Kenneth is a native of Atlanta, Georgia. He now calls Northeast Ohio home, where he has lived for the past 25 years. He enjoys exploring technology, cooking, and travelling. He is married and with two children.

Agenda

- What is Business and the Internet?
- You are a Target!
- What is Malware?
- Equifax Aftermath – What have we learned?
- Summary

Along the way, I will present "How to Protect Yourself" (for the impatient)

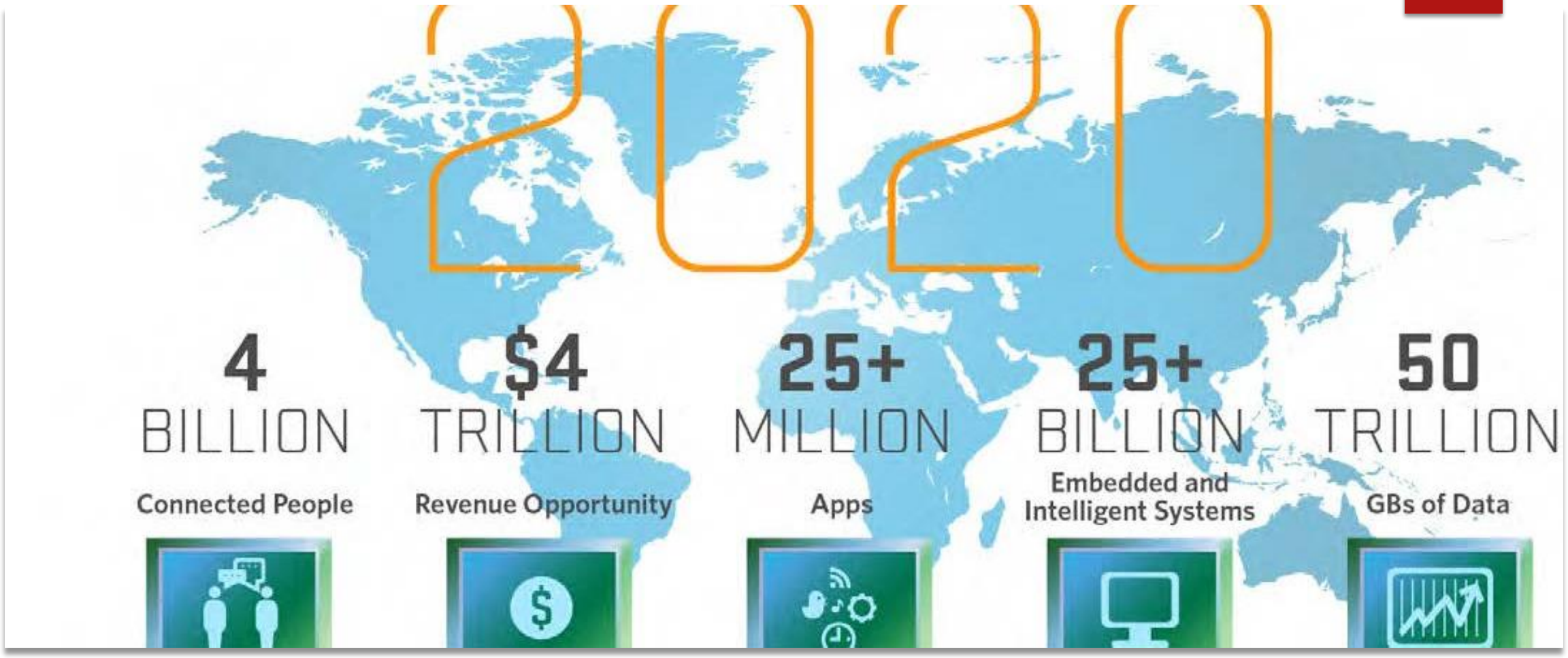
Business and the Internet

- Business uses the Internet on a daily basis
  - Commerce – Selling
  - Commerce – Buying
  - Communication and Marketing (External)
  - Workforce Communication (Internal)
  - Business Processes (Cloud Storage, Workflows, Applications)

Business and the Internet

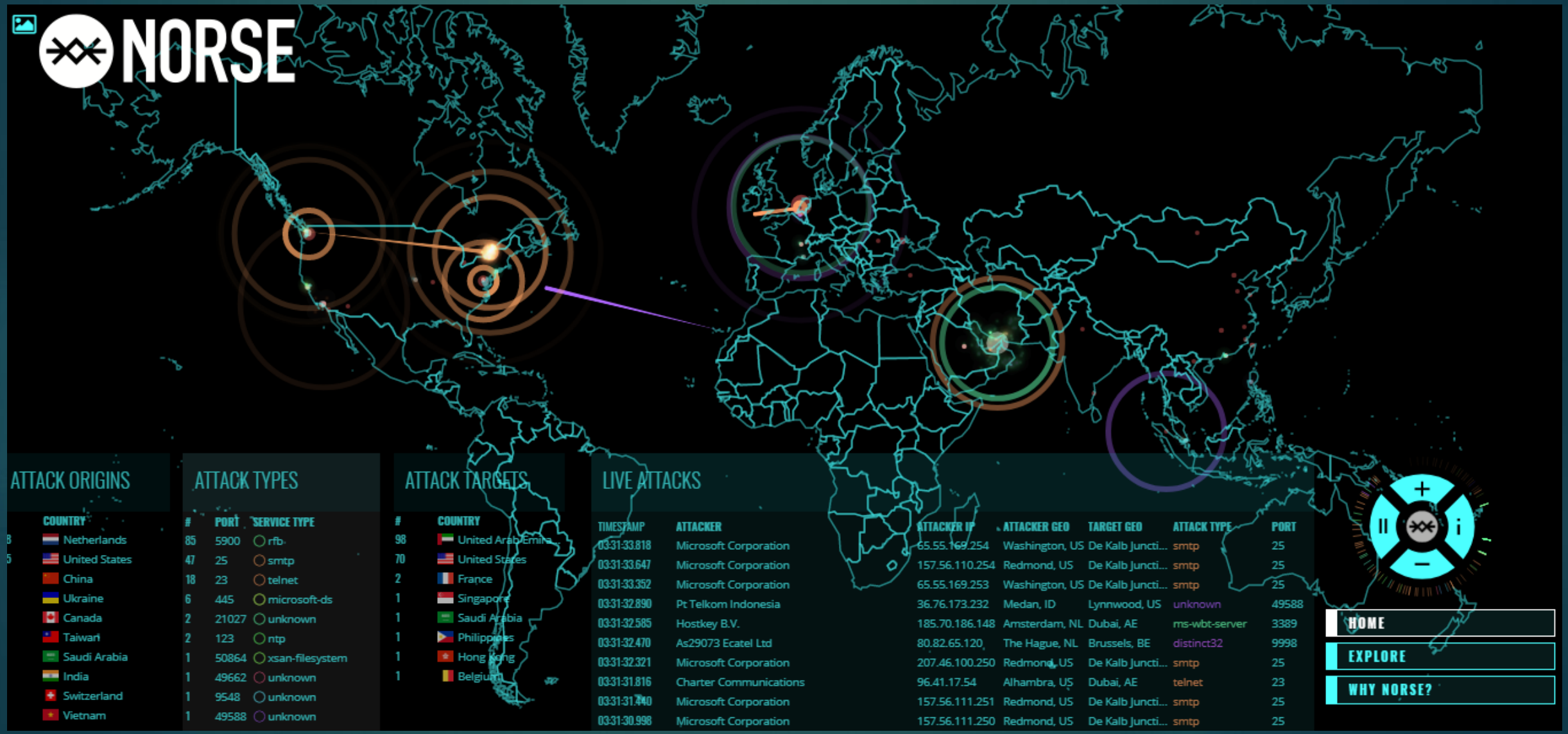
Amazon may account for 50% of all online sales this year

Apple, eBay and Walmart round out the top 4


2020
4
BILLION
Connected People
$4
TRILLION
Revenue Opportunity
25+
MILLION
Apps
25+
BILLION
Embedded and
Intelligent Systems
50
TRILLION
GBs of Data

Internet Activity

Internet Activity



You are a Target

HUMAN HACKING

Top 7 Human Risks

- Poor Password Security/Password Reuse
- Phishing
- Failing to patch or update devices/Poorly Configured Devices (BYOD)
- Insecure use of mobile media
- Sharing too much on Social Media
- Not realizing you are a Target
- Accidentally disclosing or losing data

Source: SANS Security Awareness

Top 7 Human Risks

- **Poor Password Security/Password Reuse**
- **Phishing**
- Failing to patch or update devices/Poorly Configured Devices (BYOD)
- Insecure use of mobile media
- Sharing too much on Social Media
- Not realizing you are a Target
- Accidentally disclosing or losing data

Source: SANS Security Awareness

Username & Passwords

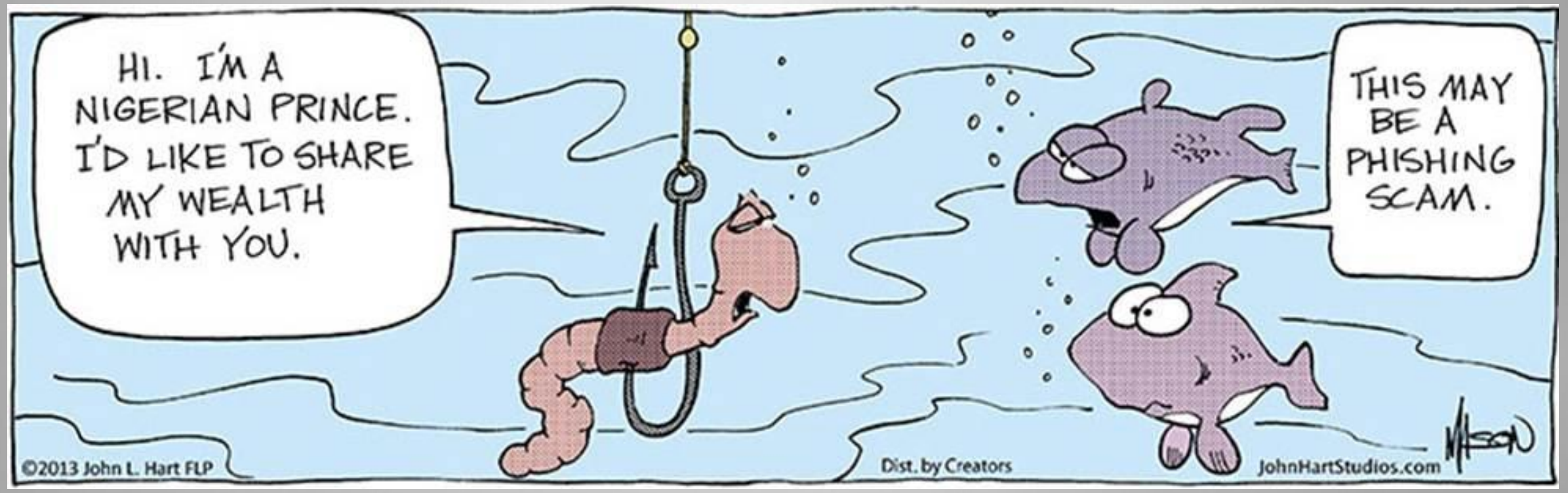
Guard email and other accounts with strong passwords

- Avoid using dictionary words, names of children or other personal information
- Make them long (phrases or sentences) that mix uppercase and lowercase letters, numbers and symbols
- Avoid using the same password everywhere
  - If its stolen, all accounts that use that password are at risk
- Make it easy to remember!
- Change it often (once a year at least!)
- It's okay to store passwords on password management system

Phishing - Don't Get Hooked

- Phishing is a social engineering/ psychological attack used by cyber criminals to trick you into giving up information or taking some action.
- Phishing originally described email attacks that would steal your online username and password.
- However the term has evolved and refers to almost any message-based attack.

Phishing


HI. I'M A NIGERIAN PRINCE. I'D LIKE TO SHARE MY WEALTH WITH YOU.
THIS MAY BE A PHISHING SCAM.
©2013 John L. Hart FLP
Dist. by Creators
JohnHartStudios.com

Phishing

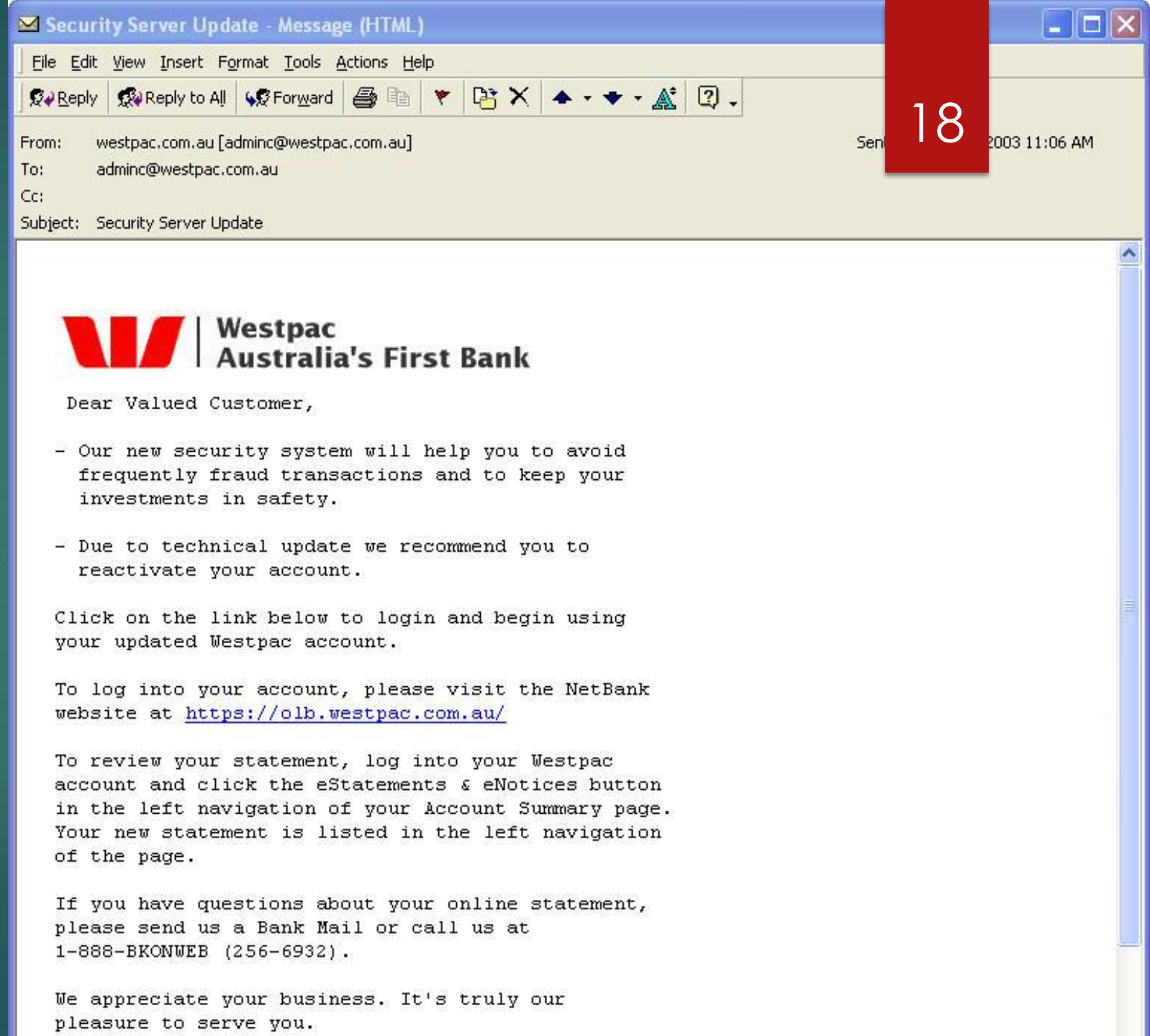
- Types of Attacks
  - **Spam** – Broad attack using Generic Email, typically has no personal information about the target
  - **Spear** – Narrow attack using some personal information about the target
  - **Whaling** – A Spear Phish against a high-profile target (executives)

Phishing Attacks

- Psychology used in a Phish
  - **Reward** - Offer "free" gifts, prizes or vacations, or exclaim, "You're a winner!"
  - **Curiosity** – Offers of "can't miss" deals
  - **Empathy/Sympathy** - Appear to be from friends or family members, but the message is written in a style not usually used by that person
  - **Fear** - Sets ultimatums such as "your account will be closed"

Phishing – Social Engineering

- Social-engineering schemes use ‘spoofed’ emails to lead customers to counterfeit websites



Security Server Update - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply Reply to All Forward

From: westpac.com.au [adminc@westpac.com.au]
To: adminc@westpac.com.au
Cc:
Subject: Security Server Update

Sen 2003 11:06 AM

Westpac
Australia's First Bank

Dear Valued Customer,

- Our new security system will help you to avoid frequently fraud transactions and to keep your investments in safety.

- Due to technical update we recommend you to reactivate your account.

Click on the link below to login and begin using your updated Westpac account.

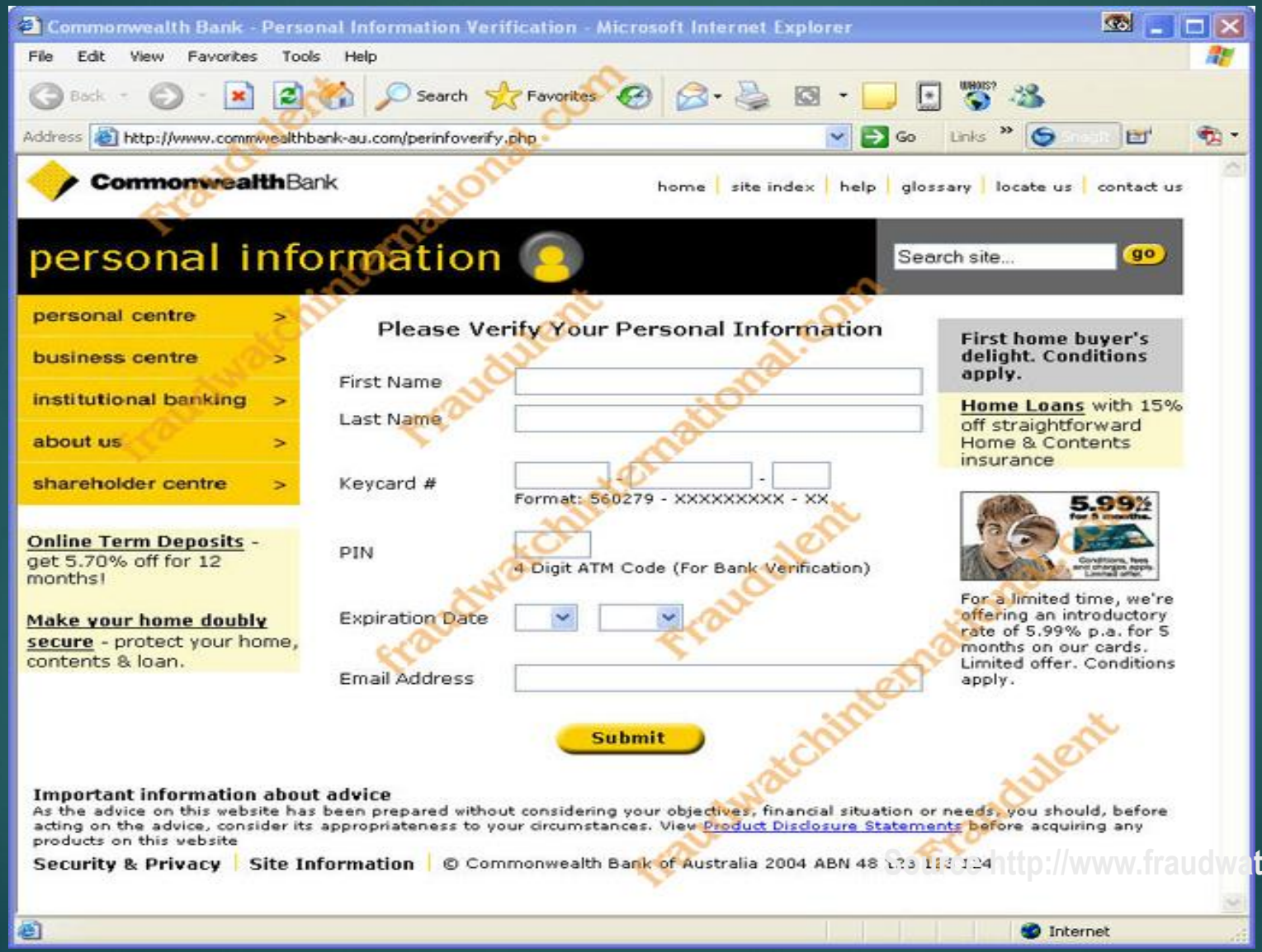
To log into your account, please visit the NetBank website at https://olb.westpac.com.au/

To review your statement, log into your Westpac account and click the eStatements & eNotices button in the left navigation of your Account Summary page. Your new statement is listed in the left navigation of the page.

If you have questions about your online statement, please send us a Bank Mail or call us at 1-888-BKONWEB (256-6932).

We appreciate your business. It's truly our pleasure to serve you.

Phishing – Social Engineering



Countermeasures

- **Education!** Educate employees to never respond to request for personal information from your bank or health insurance provider that comes via an email hyperlink
- **Policy!** Educate your employees to never respond to any Email with corporate information without verification

Protecting your Computer

- How do I protect my computer
  - Make sure that you routinely delete Internet Temp Files, History or Cookies from your browser software.
  - Make sure you have up to date firewall and antivirus software on every computer you work on.
  - Turn off or limit any file sharing on your systems.
  - Do not install unnecessary software (games) on your business computers
  - Password protect all accounts on all systems. Use good passwords and secure your passwords!

What is Malware?

- Malicious Code
  - Viruses
  - Trojan horses
  - Spyware
  - Adware
  - Ransomware
  - Worms
  - Zombies and botnets

What is Malware?

- Malicious Code
  - **Viruses**
  - Trojan horses
  - **Spyware**
  - **Adware**
  - **Ransomware**
  - Worms
  - Zombies and botnets

What is a Virus?

- A *virus* is a program that attempts to damage a computer system and replicate itself to other computer systems.
- A virus has the following characteristics:
  - A virus requires a *replication* mechanism which is a file that it uses as a host. When the host file is distributed, the virus is also distributed.
  - Viruses typically attach to files with execution capabilities such as .doc, .exe, and .bat extensions.
  - Many viruses are distributed via e-mail and are distributed to everyone in your address book.
  - The virus only replicates when an *activation* mechanism is triggered. For example, each time the infected file or program is executed, the virus is activated.
    - The virus is programmed with an *objective*, which is usually to destroy, compromise, or corrupt data.

Spyware

- *Spyware* is software that is installed without the user's consent or knowledge, designed to intercept or take partial control over the user's interaction with the computer.
- Spyware:
  - Is installed on your machine by visiting a particular Web page or running a particular application.
  - Collects various types of personal information, such as Internet surfing habits and passwords, and sends the information back to its originating source.
  - Uses tracking cookies to collect and report a user's activities.
  - Can interfere with user control of the computer such as installing additional software, changing computer settings, and redirecting Web browser activity.

Adware

- *Adware* monitors actions that denote personal preferences, and then sends pop-ups and ads that match those preferences.
- Adware:
  - Is usually passive.
  - Is privacy invasive software.
  - Is installed on your machine by visiting a particular Web site or running an application.
  - Is usually more annoying than harmful.

What is Ransomware?

- Ransomware is a form of malware that infects computers and restricts users access
- This malware in some instances has issued threats to permanently delete the users files unless they pay hundreds or even thousands of dollars
- Ransomware has been around for several years
- There has been a definite increase in its use by cyber criminals

Who does Ransomware impact?

Ransomware impacts more than home computers

Many businesses, financial institutions, government agencies and academic institutions have become infected

In some instances these organizations lost sensitive or proprietary information, disruption to regular operations and financial loss

How do you become infected?

Early ransomware infections came from infected email attachments

More recently the malware is coming from infected websites via a technique called a drive-by download

A user becomes infected by simply clicking on a compromised website, lured there by a deceptive email or pop-up window

Latest Ransomware Threats

- CryptoWall and CryptoWall 2.0 are making their rounds
  - This malware encrypts files on a computers harddrive and any external or shared drives to which the computer has access
  - The malware directs the user to a personalized victim ransom page that contains the initial ransom amount
    - Anywhere from $200 to $5000 dollars
  - According to US CERT these infections can be devastation and difficult to recover from

Latest news

- Law enforcement officials have seized the Cryptolocker command and control servers.
- The investigation continues into thee criminals behind Cryptolocker, but the malware is unable to encrypt any additional computers

- Then something new arrived
  - WannaCry
  - Petya (Ukraine/Europe)

What is the WannaCry ransomware attack?

- Began on May 12 but leverages previously known exploits
- Infiltrates endpoints and encrypts all the files, demanding a ransom payment $300 USD in bitcoin
- Exploits a known Windows vulnerability that enables remote code execution
  - Microsoft Windows patch was available in March; those who didn't address this patch are vulnerable
- Crippled at least 100K organizations across multiple industries in over 150 countries
- 200K+ infected endpoints

What makes WannaCry so sophisticated?

- The malware uses highly potent NSA exploits that were allegedly leaked by "ShadowBrokers" in April 2017
- Exploits a flaw in the Server Message Block (SMB) that enables it's worm-like propagation
- Uses strong, asymmetric encryption, employing the RSA 2048-bit cipher to encrypt files
- Uses a modular architecture which is used in legitimate software and in complex malware projects like banking trojans

Paying the Ransom

- Early ransomware scams required payment via pre-paid credit cards
- Victims now are being asked to pay in Bitcoin, a decentralized virtual currency

Ransomware is expanding

- A growing problem is ransomware that locks down mobile phones and demands payment to unlock them

Protect your computer from Ransomware

- Currently making sure you have the lasted updates antivirus software installed on your computer
- Avoid being a victim of a Phishing Attack, which is typically how Ransomware gets into the network
- Avoid using your personal/business device on trips outside of the United States
  - Use a "burner" device, stripped of sensitive, personal information and has only "what you need" for the trip
  - Wipe the "burner" device before coming back to your corporate network

Fake AV

- FakeAV or **Fake** AntiVirus, also known as Rogue AntiVirus, Rogues, or ScareWare, is a class of malware that displays false alert messages to the victim concerning threats that do not really exist.

Equifax Aftermath: Lessons Learned

Equifax and History of Data Breaches

- Who here is scrambling around in the aftermath of the recent breach at Equifax to figure out if you've been compromised?
- Note: 143 million records were stolen from Equifax.
- Even if you weren't one of the 143 million, your information may have been lost in the previous breaches:
  - Kansas Department of Commerce – 5 million records
  - Office of Personnel Management – 21.5 million records
  - Target – 40 million credit cards, 70 million records
  - Home Depot – 56 million credit card, 53 million email addresses
  - JP Morgan Chase – 76 million households, 7 million businesses
  - Anthem Health Insurance – 80 million records
  - Heartland – 130 million credit cards

What could happen?

- The Equifax breach gave criminals access to vital personal information, including names, social security numbers, birthdates, addresses, and in some cases, driver's license IDs and credit card numbers. And here's just a slice of what thieves can do with that data:
  - Open financial accounts
  - Apply for credit cards, mortgages, and other financial services
  - Get medical care at your expense
  - File for a tax refund in your name
  - Get a job in your name and let you pay the taxes
  - Steal your benefits
  - All of the above (aka, identity theft)

Steps to protect yourself

- **Best recommendation**: freeze your credit immediately with all four of the major credit bureaus. By freezing your credit, you'll prevent criminals from trying to open up new accounts in your name—all of your current credit cards will still work.
- Three things you'll want to know before contacting the credit bureaus.
  1. You'll want to pull a credit report. It doesn't matter if you've already frozen your accounts, you can still monitor using the free tool.
     - It is recommend that you pull only one report now, then periodically pull one every three months.
     - https://www.annualcreditreport.com/requestReport/getNextReport.action
  2. The cost to freeze your credit report is minimal…typically a one-time fee of $10 per bureau.
  3. You must set or receive PINs when freezing your credit. Save these in a secure location, whether that's using a password manager or physically storing the printed PIN paper someplace safe and out of sight.

Where to go to freeze your credit

- Equifax: (800) 685-1111 or https://www.freeze.equifax.com/
- Experian: (888) 397-3742 or https://www.experian.com/ncaconline/freeze
- TransUnion: (888) 909-8872 or https://freeze.transunion.com/
  - Note: their phone prompts move quickly, so have your newly thought-up PIN and credit card information readily available.
- Innovis: (800) 540-2505 or https://www.innovis.com/securityFreeze

Additional monitoring services

- The use of monitoring services is not a bad idea. However, choose your service wisely.
- Note some services just monitor…others add the benefit of "helping" you out of trouble if identity theft occurs.
- None are "fool proof".

Summary

- If you're affected by the Equifax breach, you have a heightened risk of becoming a victim of identity theft.
- One new credit card created by an attacker in your name is going to cause a massive headache.
- Better to stay ahead of it than spend the next month trying to clean up from identity theft.
- Realize that you are a target! And that you are *already* a victim!
- Set good business policies on Internet use. Secure your valuable assets – YOUR DATA!
- Be ever vigilant and stay safe.

Summary

Be ever vigilant and stay safe.