

Protecting Your Home Computer



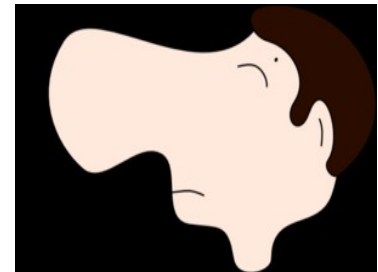
SIR A2CAT, November 19, 2015

<http://alanbaker.net/presentations/protecting.pdf>

Alan Baker

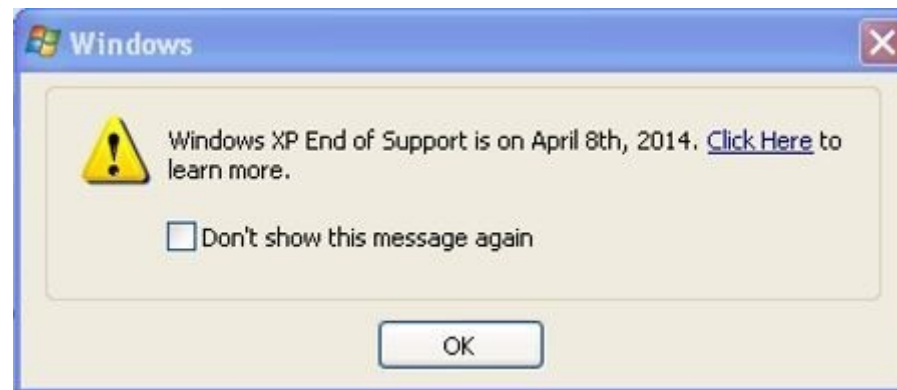
Protecting your Home Computer

- **Attacks – why and how**
- **Top Online Safety Practices**
- **Defenses**



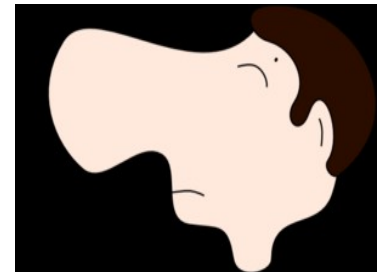
Attacks—why and how

- “Follow the money”
- Social engineering: “Hello, this is Microsoft.”
- Malware in email, software, or web sites
- **Unpatched software vulnerabilities**



Protecting your Home Computer

- Attacks – why and how
- **Top Online Safety Practices**
- Defenses



Which column is better?

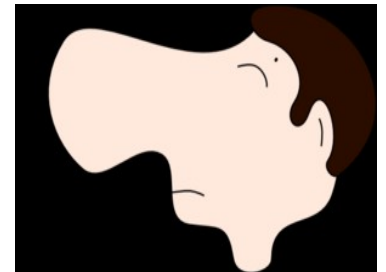
TOP ONLINE SAFETY PRACTICES		VS	TOP ONLINE SAFETY PRACTICES	
1. USE ANTIVIRUS SOFTWARE				1. INSTALL SOFTWARE UPDATES
2. USE STRONG PASSWORDS				2. USE UNIQUE PASSWORDS
3. CHANGE PASSWORDS FREQUENTLY				3. USE TWO-FACTOR AUTHENTICATION
4. ONLY VISIT WEBSITES THEY KNOW				4. USE STRONG PASSWORDS
5. DON'T SHARE PERSONAL INFORMATION				5. USE A PASSWORD MANAGER

Non-experts vs. Security Experts

SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES	VS	SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES
1. USE ANTIVIRUS SOFTWARE 		1. INSTALL SOFTWARE UPDATES 
2. USE STRONG PASSWORDS 		2. USE UNIQUE PASSWORDS 
3. CHANGE PASSWORDS FREQUENTLY 		3. USE TWO-FACTOR AUTHENTICATION 
4. ONLY VISIT WEBSITES THEY KNOW 		4. USE STRONG PASSWORDS 
5. DON'T SHARE PERSONAL INFORMATION 		5. USE A PASSWORD MANAGER 

Protecting your Home Computer

- Attacks – why and how
- Top online safety practices
- **Defenses**



Simple Defenses

- Use a non-administrator account.
- Install Microsoft EMET
- Uninstall programs you don't use (Java?)
- **Automatic** software updates to
 - Operating System (Mac OS, Windows)
 - Adobe Flash, Reader, Acrobat
 - Web browser (IE, Chrome, Firefox)
 - Antivirus (**one** unexpired program)

Passwords

- Weak passwords

- Words, patterns

P@\$\$WORD

- Strong passwords

- MiXeD cAsE + numbers + special characters
- Sentence acronym: EbiO11&KbiO23
- DO NOT REUSE PASSWORDS.
- How to remember them? Computer? Paper?

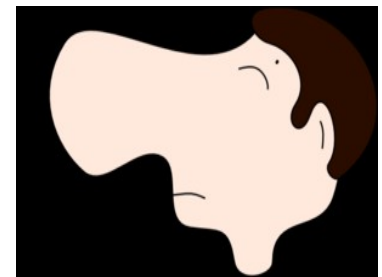
- Password managers

- LastPass, Dashlane, KeePass

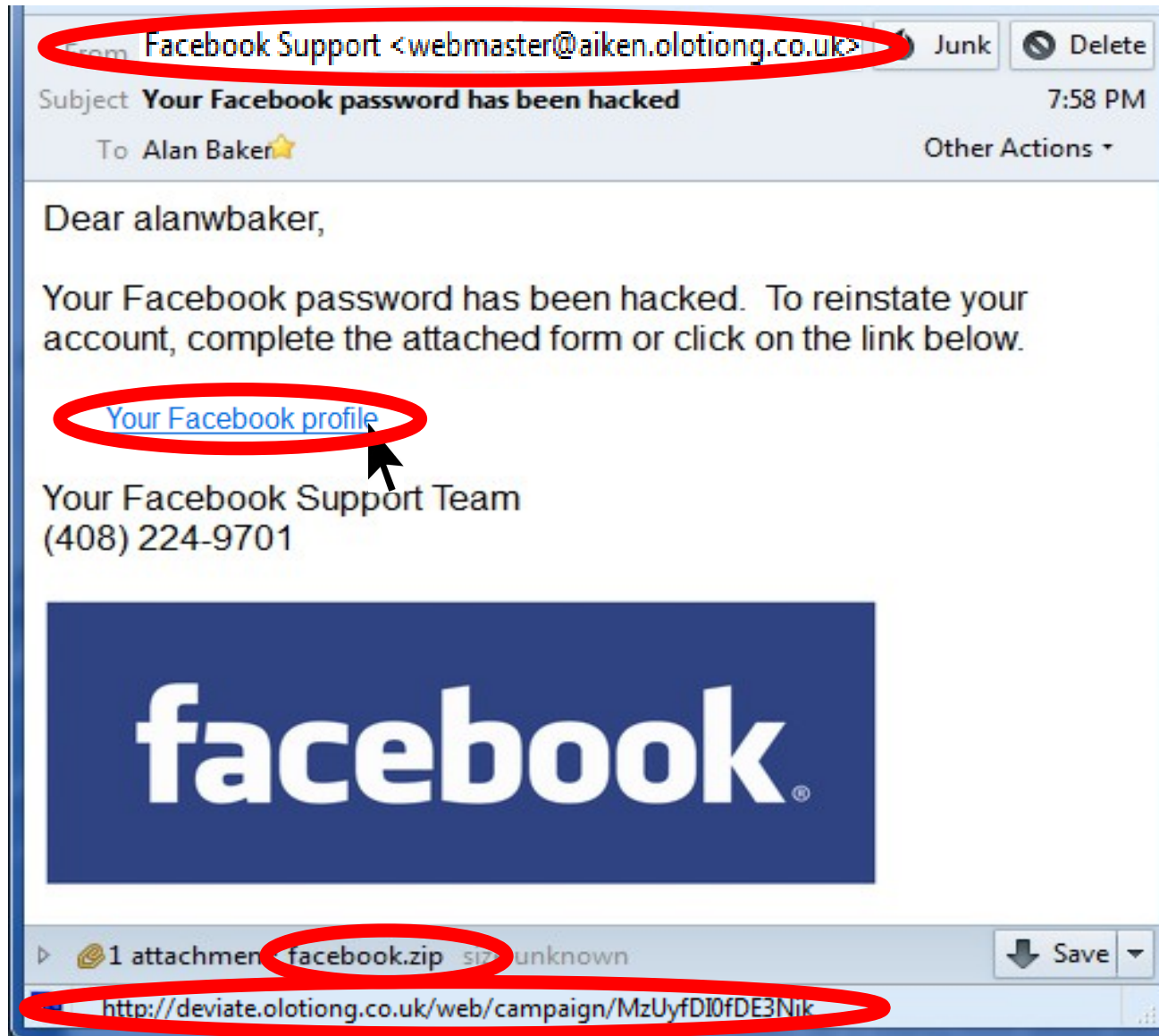


Phishing

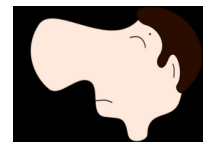
- The sniff test
- Recognize phishing emails
 - Attachment extension is .zip, .exe, or .doc
 - Link to a web site you do not know
 - Sender name and email address



Phishing Email



Alan Baker



Another Phishing Email

- Turn on full headers

Subject: INCOMING FAX REPORT : Remote ID: 3153096150

From: Administrator <administrator@sjpc.org>

Date: 2/10/2014 7:06 AM

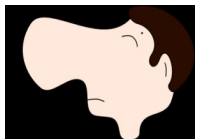
To: <beberly@sjpc.org>, <baker@sjpc.org>, <buoysandgulls@sjpc.org>, <bmurray@sjpc.org>

Return-path: <no-reply@occsb.com>

Envelope-to: baker@sjpc.org

Delivery-date: Mon, 10 Feb 2014 08:07:01 -0700

Received: from legrand-noisy.pck.nerim.net ([62.212.96.114]:51951) by slan-550-69.annosting.com with esmtp (Exim 4.82) (envelope-from <no-reply@occsb.com>)



How do I find malware?

- Control Panel: Programs and Features
 - Sort by installation date
- Command prompt: msconfig
 - Startup tab
- Web browser add-ons
 - Extensions, plug-ins, toolbars



What will you do when you see this?

Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **10/06/14 - 09:14** the cost of decrypting files will increase **2** times and will be **1000 USD/EUR**

Prior to increasing the amount left:
119h 58m 24s

Your system: **Windows 7 (x64)** First conned IP:   Total encrypted **28** files.

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

- Cryptowall: a cautionary tale

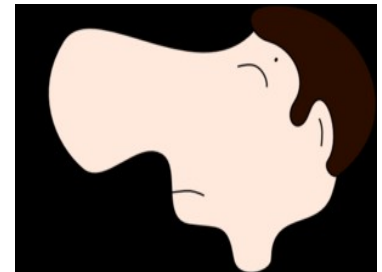
Backup and recovery

- Use real backup software
- Back up the whole computer (system & files)
- To an external disk drive
- Then disconnect it



Protecting your Home Computer

- Attacks - why and how
- Top Online Safety Practices
- Defenses



Protecting Your Home Computer



You can download this presentation from
<http://alanbaker.net/presentations/protecting.pdf>

Alan Baker
baker@alanbaker.net