10 STEPS FOR SECURING YOUR DIGITAL IDENTITY

Peter Pelland, CEO & Founder, Pelland Advertising

1. KEEP YOUR PASSWORDS SECURE

KEEP YOUR PASSWORDS SECURE

- What is secure? Characters? Length?
- Use a unique password for each and every site.
- Change passwords and security questions frequently.
- Change compromised passwords, change weak passwords, change reused passwords, change old passwords.
- Take the test: https://howsecureismypassword.net/

KEEP YOUR PASSWORDS SECURE

- Use a secure password generator to create a unique random password for every site you visit. Use the highest character standards that the sites allow, by default including upper- and lower-case characters, numbers, and symbols. A good habit is to use a minimum of 16 characters, more for online banking and sites where you enter highly secure information.
- Secure Password Generator is an excellent resource. https://passwordsgenerator.net/

KEEP YOUR PASSWORDS SECURE

- Use a password safe, with one highly secure master password.
- LastPass - https://www.lastpass.com/
- Dashlane - https://www.dashlane.com/
- Keeper - https://keepersecurity.com/

These all work with Windows, Mac, iOS, and Android operating systems; have plugins for popular browsers; include two-factor authentication; include form-filling; offer fingerprint login on mobile devices; and have free versions.

JANUARY 29, 2018

This is the date when the Internal Revenue Service started accepting 2017 individual tax returns, and when filers were urged to submit their returns as early as possible after 143,000,000 households were victims of the widely publicized Equifax security breach. The compromised data included names, dates of birth, Social Security numbers, addresses, and driver’s license numbers.

According to Statista, there were about 126.22 million households in the United States in 2017. In other words, EVERY household in America had its personal security violated.

2. UPDATE YOUR SOFTWARE

UPDATE YOUR SOFTWARE

The Equifax security breach was the result of **1 software patch** that the company knew should have been installed but postponed doing so. The company then waited 6 weeks to disclose the breach. The company's CEO was forced to resign, its reputation is forever tarnished, and it had a multi-million dollar no-bid contract to provide "taxpayer identity" services to the Internal Revenue Service suspended in October 2017.

Could your small business survive if it was held accountable for a similar – but much smaller – security breach?

UPDATE YOUR SOFTWARE

You have responsibilities to your business AND its customers.

The most vulnerable software on your computers and phones includes:

- The **operating system** *(apply the latest updates!)* Support for Windows Vista ended on April 10, 2012; support for Windows 7 ended on January 13, 2015; and support for Windows 8/8.1 ended on January 9, 2018.
- Browsers *(always run the latest version!)*
- Adobe Reader and Adobe Flash Player *(apply the latest updates!)*

UPDATE YOUR SOFTWARE

You have responsibilities to your business AND its customers.

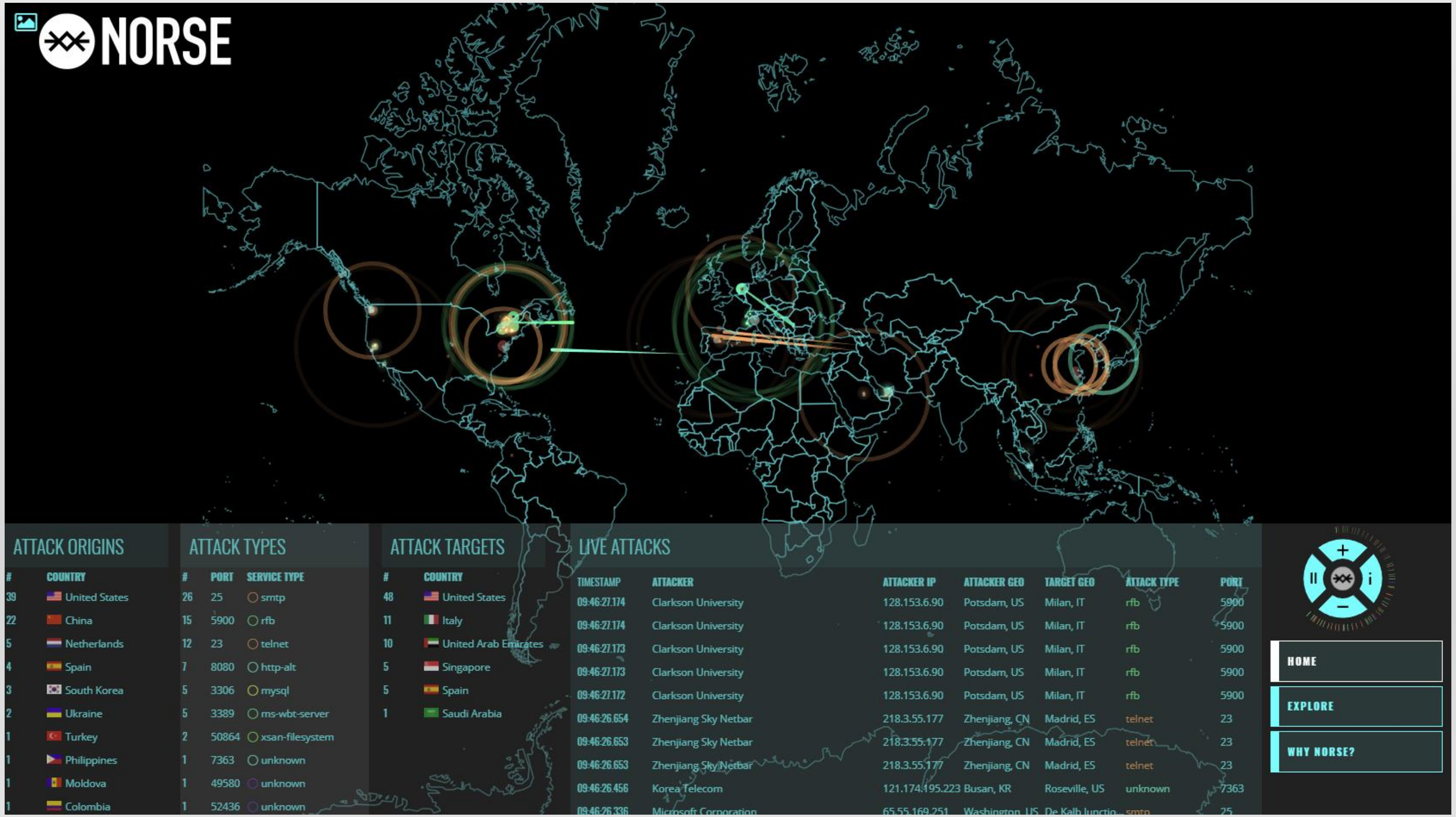
The most vulnerable software on your computers and phones includes:

- Java *(apply the latest updates!)*
- Software firewalls.
- Anti-virus software.

Is your anti-virus software reliable and updated daily?

UPDATE YOUR SOFTWARE

Hack attacks are continuous and ongoing. Take a look at a real-time map of cyber attacks: http://www.norse-corp.com/



ATTACK ORIGINS

#	COUNTRY
39	United States
22	China
5	Netherlands
4	Spain
3	South Korea
2	Ukraine
1	Turkey
1	Philippines
1	Moldova
1	Colombia

ATTACK TYPES

#	PORT	SERVICE TYPE
26	25	○ smtp
15	5900	○ rfb
12	23	○ telnet
7	8080	○ http-alt
5	3306	○ mysql
5	3389	○ ms-wbt-server
2	50864	○ xsan-filesystem
1	7363	○ unknown
1	49580	○ unknown
1	52436	○ unknown

ATTACK TARGETS

#	COUNTRY
48	United States
11	Italy
10	United Arab Emirates
5	Singapore
5	Spain
1	Saudi Arabia

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
09:46:27.174	Clarkson University	128.153.6.90	Potsdam, US	Milan, IT	rfb	5900
09:46:27.174	Clarkson University	128.153.6.90	Potsdam, US	Milan, IT	rfb	5900
09:46:27.173	Clarkson University	128.153.6.90	Potsdam, US	Milan, IT	rfb	5900
09:46:27.173	Clarkson University	128.153.6.90	Potsdam, US	Milan, IT	rfb	5900
09:46:27.172	Clarkson University	128.153.6.90	Potsdam, US	Milan, IT	rfb	5900
09:46:26.654	Zhenjiang Sky Netbar	218.3.55.177	Zhenjiang, CN	Madrid, ES	telnet	23
09:46:26.653	Zhenjiang Sky Netbar	218.3.55.177	Zhenjiang, CN	Madrid, ES	telnet	23
09:46:26.653	Zhenjiang Sky Netbar	218.3.55.177	Zhenjiang, CN	Madrid, ES	telnet	23
09:46:26.456	Korea Telecom	121.174.195.223	Busan, KR	Roseville, US	unknown	7363
09:46:26.336	Microsoft Corporation	65.55.169.251	Washington, US	De Kalb Junctio...	smtp	25

3. BE CAREFUL OPENING EMAIL!

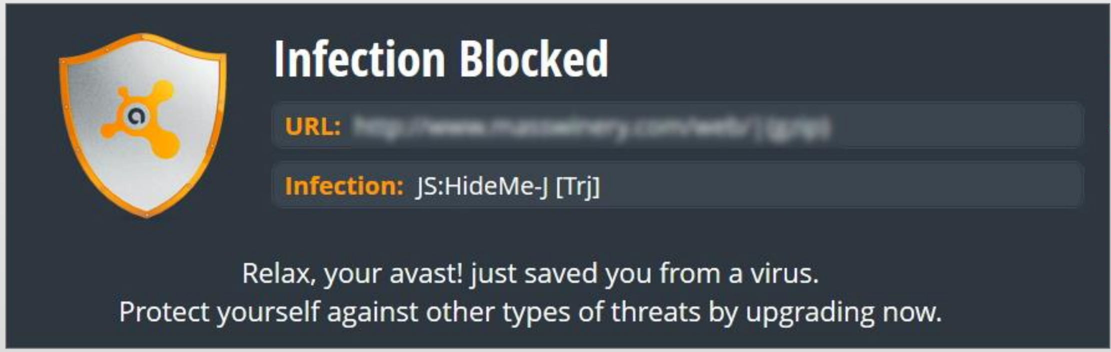
BE CAREFUL OPENING EMAIL!

Be particularly wary of links and unexpected attachments!

- **Sending addresses can be easily faked** (just like the numbers that appear on your phone’s caller ID.)
- Carefully **check the spelling** of sender addresses and links.
- **Hover over links** before even thinking of clicking! The link that appears and the actual destination may not be the same.
- Beware of suspicious content and spelling errors.
- Flag spam to help your email provider to better recognize it.
- Check your spam folder for legitimate messages.

4. BE CAREFUL BROWSING

Ever see warnings like this? Be glad if you did!

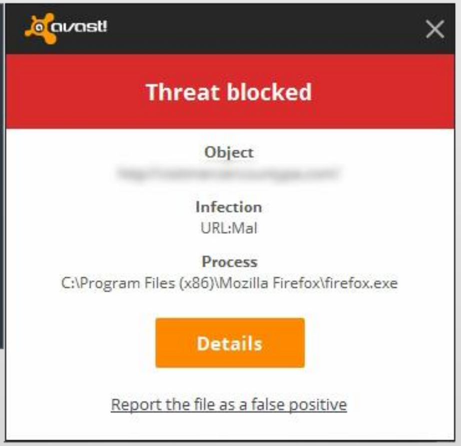


Infection Blocked

URL: [redacted]

Infection: JS:HideMe-J [Trj]

Relax, your avast! just saved you from a virus.
Protect yourself against other types of threats by upgrading now.

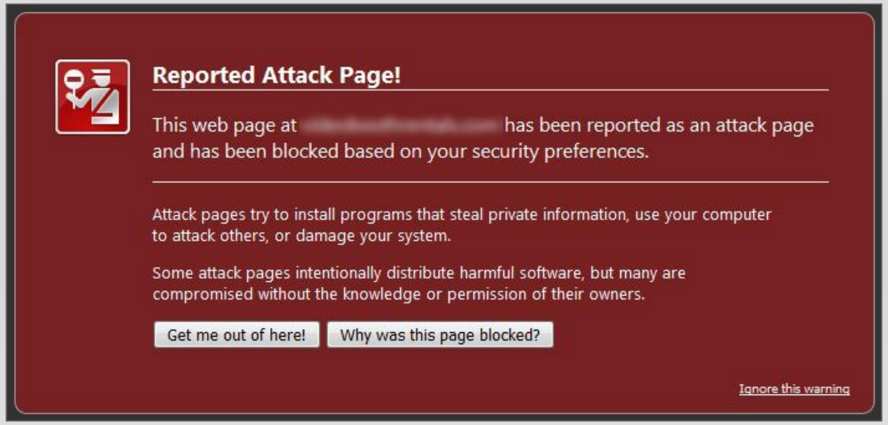


Threat blocked

Object
[redacted]

Infection
URL:Mal

Process
C:\Program Files (x86)\Mozilla Firefox\firefox.exe

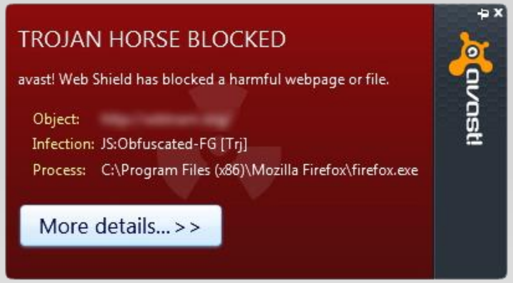


Reported Attack Page!

This web page at [redacted] has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.



TROJAN HORSE BLOCKED

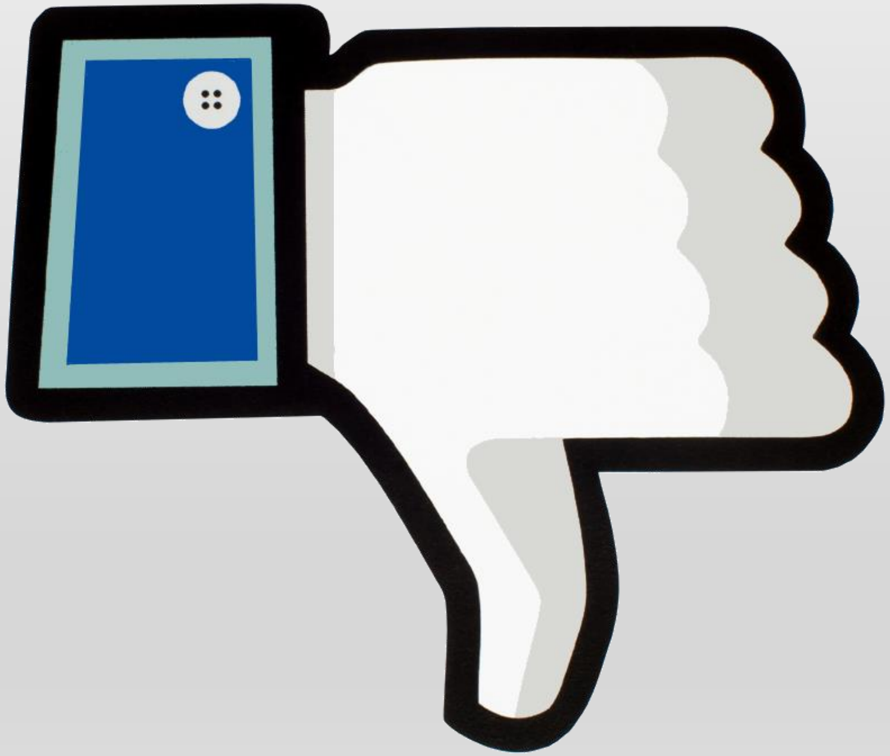
avast! Web Shield has blocked a harmful webpage or file.

Object: [redacted]
Infection: JS:Obfuscated-FG [Trj]
Process: C:\Program Files (x86)\Mozilla Firefox\firefox.exe

BE CAREFUL BROWSING

- Type in URLs very carefully. Online **thieves often register similar domain names**, with one character out of place.
- It is very easy to build a fake version of what otherwise appears to be a known (and trusted) website.
- Look for the **https** protocol that identifies a secure site.
- **Do not click on links or download files** that are executable or could contain malicious code. (These include .exe files and Word documents.)
- Never ask your browser to remember passwords.
- Always run real-time AV and malware protection.

5. THE ANTI-SOCIAL MEDIA



THE ANTI-SOCIAL MEDIA

If you are a user of the social media, particularly Facebook, be aware that you are continually compromising your personal privacy.

- The intrusions go far beyond being showed advertising based upon your posts, comments, and “likes”. We now know that ads have even been used to undermine our elections and the democratic process.
- Adjust your security settings – frequently.
- Never blindly share content without checking its authenticity.
- Never enter contests or take “tests” that involve divulging your personal information.

THE ANTI-SOCIAL MEDIA

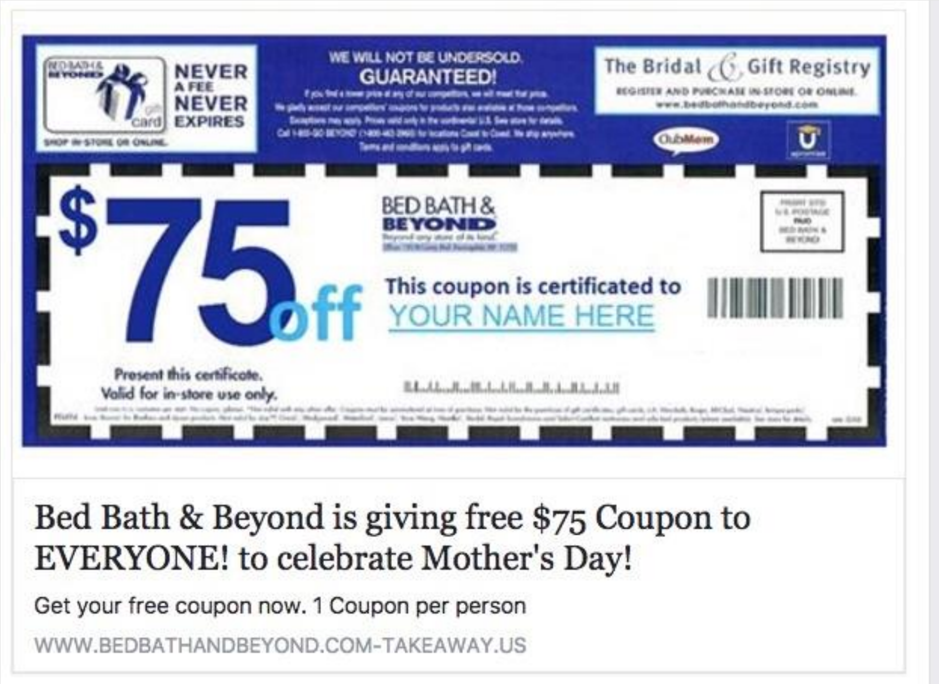
Most “tests” and quizzes on Facebook that appear to be innocent fun are *at minimum* harvesting your personal information for marketing purposes.

Some purport to determine your intelligence level, your true nationality, where you would actually prefer to live, where you belong in history, or other nonsense. To determine the “answer”, you will be asked questions like where you lived as a child, your mother’s maiden name, the name of your first pet, and so forth.

These are the same questions and answers that are often used to protect your online security!

THE ANTI-SOCIAL MEDIA

Beware of coupons, contests, and offers that are too good to be true – arriving on Facebook or your email. Clicking through to the links could make you anything but a winner.



BED BATH & BEYOND gift card NEVER A FEE NEVER EXPIRES

SHOP IN-STORE OR ONLINE.

WE WILL NOT BE UNDERSOLD. GUARANTEED!

If you find a lower price at any of our competitors, we will meet that price. We gladly accept our competitors' coupons for products also available at those competitors. Exceptions may apply. Prices valid only in the continental U.S. See store for details. Call 1-800-GO BEYOND (1-800-462-3966) for locations Coast to Coast. We ship anywhere. Terms and conditions apply to gift cards.

The Bridal & Gift Registry

REGISTER AND PURCHASE IN-STORE OR ONLINE.
www.bedbathandbeyond.com

$75 off

BED BATH & BEYOND
Beyond any store of its kind.

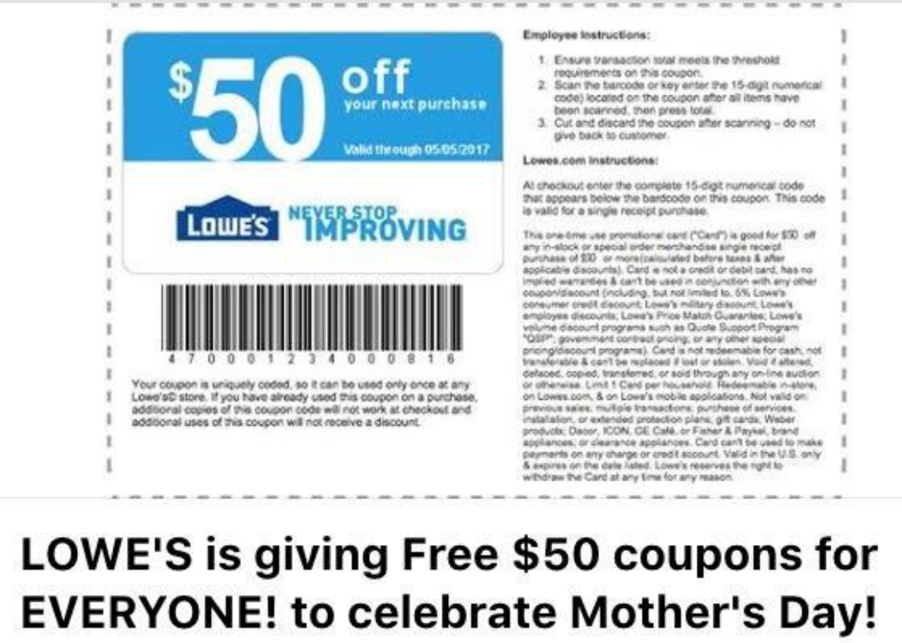
This coupon is certificated to YOUR NAME HERE

Present this certificate.
Valid for in-store use only.

Bed Bath & Beyond is giving free $75 Coupon to EVERYONE! to celebrate Mother's Day!

Get your free coupon now. 1 Coupon per person

WWW.BEDBATHANDBEYOND.COM-TAKEAWAY.US



$50 off your next purchase

Valid through 05/05/2017

LOWE'S NEVER STOP IMPROVING

4 7 0 0 0 1 2 3 4 0 0 0 8 1 6

Your coupon is uniquely coded, so it can be used only once at any Lowe's® store. If you have already used this coupon on a purchase, additional copies of this coupon code will not work at checkout and additional uses of this coupon will not receive a discount.

Employee Instructions:

1. Ensure transaction total meets the threshold requirements on this coupon.
2. Scan the barcode or key enter the 15-digit numerical code) located on the coupon after all items have been scanned, then press total.
3. Cut and discard the coupon after scanning – do not give back to customer.

Lowes.com Instructions:

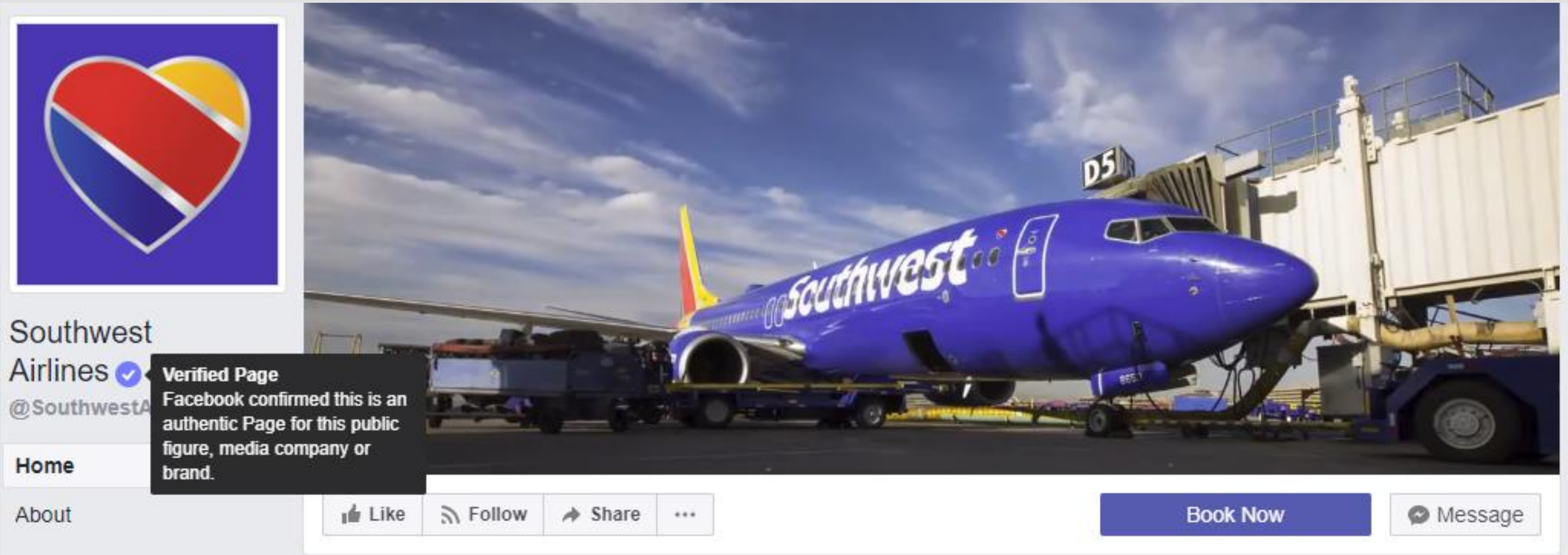
At checkout enter the complete 15-digit numerical code that appears below the bardcode on this coupon. This code is valid for a single receipt purchase.

This one-time use promotional card ("Card") is good for $50 off any in-stock or special order merchandise single receipt purchase of $50 or more(calculated before taxes & after applicable discounts). Card is not a credit or debit card, has no implied warranties & can't be used in conjunction with any other coupon/discount (including, but not limited to, 5% Lowe's consumer credit discount; Lowe's military discount; Lowe's employee discounts; Lowe's Price Match Guarantee; Lowe's volume discount programs such as Quote Support Program "QSP"; government contract pricing; or any other special pricing/discount programs). Card is not redeemable for cash, not transferable & can't be replaced if lost or stolen. Void if altered, defaced, copied, transferred, or sold through any on-line auction or otherwise. Limit 1 Card per household. Redeemable in-store, on Lowes.com, & on Lowe's mobile applications. Not valid on: previous sales; multiple transactions; purchase of services, installation, or extended protection plans; gift cards; Weber products; Dacor, ICON, GE Café, or Fisher & Paykel, brand appliances; or clearance appliances. Card can't be used to make payments on any charge or credit account. Valid in the U.S. only & expires on the date listed. Lowe's reserves the right to withdraw the Card at any time for any reason.

LOWE'S is giving Free $50 coupons for EVERYONE! to celebrate Mother's Day!

THE ANTI-SOCIAL MEDIA

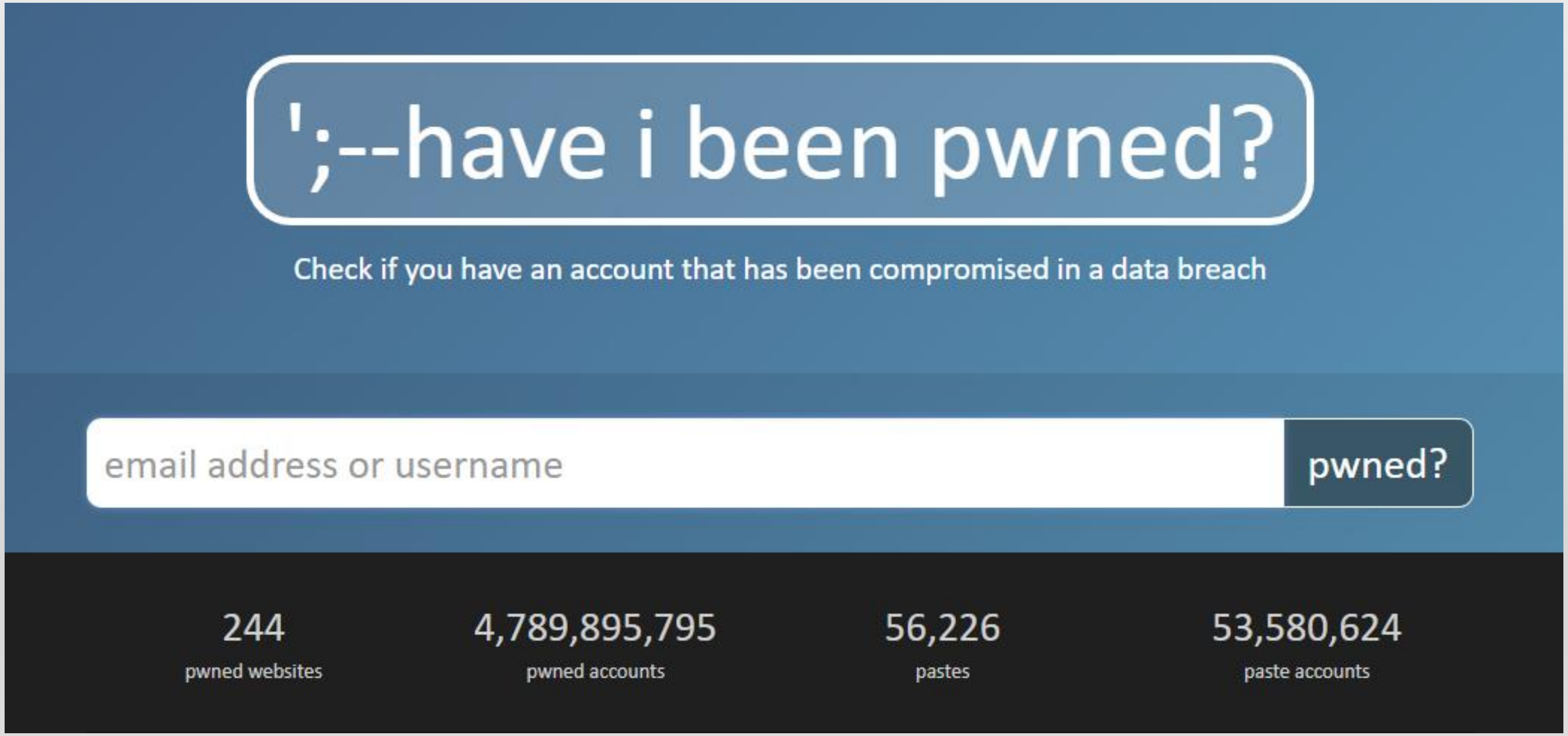
- Look for the **Verified Page checkmark** on Facebook to confirm that you are at an authentic page for a company.
- Major companies will have millions of “likes”, not just 2,047.



Verified Page
Facebook confirmed this is an authentic Page for this public figure, media company or brand.

6. TEST YOUR VULNERABILITY

https://haveibeenpwned.com/



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

244	4,789,895,795	56,226	53,580,624
pwned websites	pwned accounts	pastes	paste accounts

7. CURTAIL YOUR USE OF PUBLIC WI-FI

CURTAIL YOUR USE OF PUBLIC WI-FI

- Never use public Wi-Fi that is not secured with a password.
- Turn off automatic Wi-Fi connectivity on your phone, seeking hotspots.
- Use a Virtual Private Network, or VPN, when accessing a remote network.
- Visit only sites with https encryption.
- Do not use a public network to access your online banking, healthcare, or to shop online.
- If you must, implement two-factor authentication when logging into sensitive sites.

8. WHAT ABOUT YOUR OWN WEBSITE?

homestead®

WiX.com

vistaprint®

GoDaddy.COM WebsiteBuilder

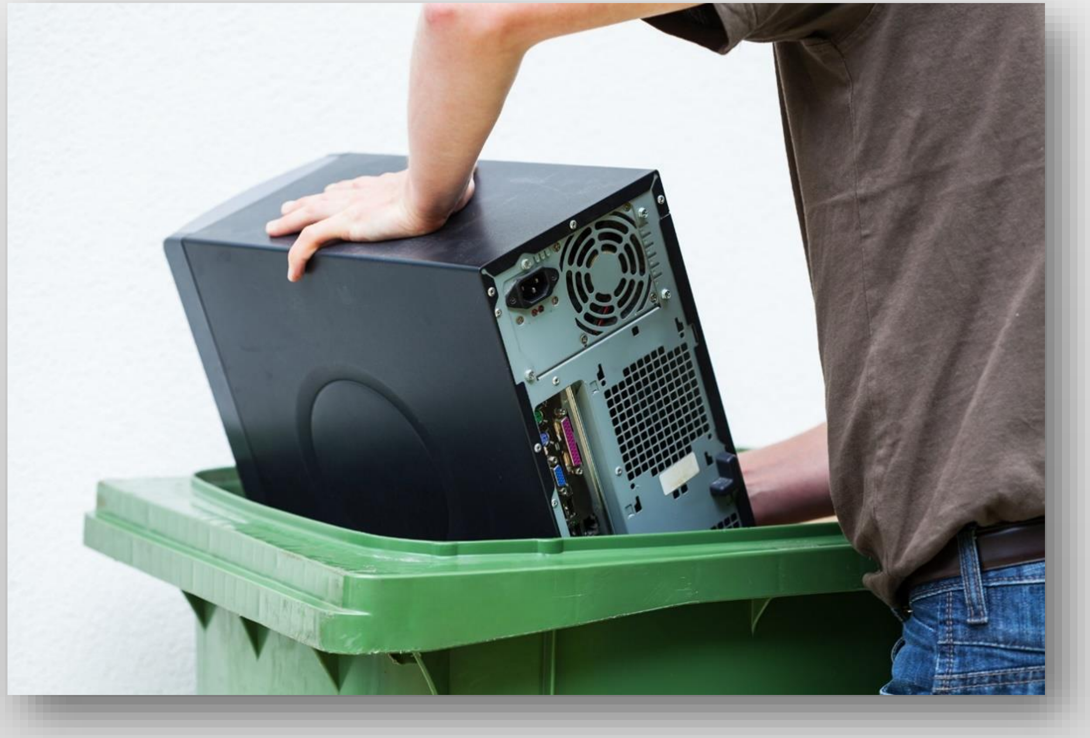
weebly

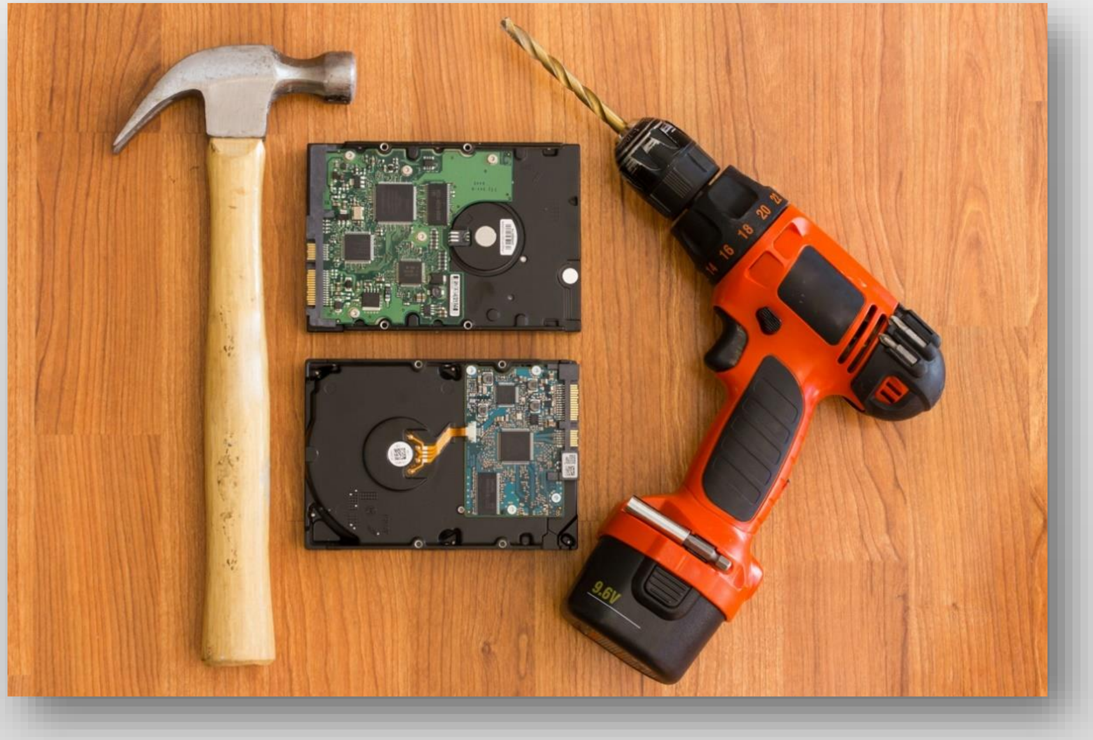
WHAT ABOUT YOUR OWN WEBSITE?

You have a responsibility to avoid compromising the security of visitors. Equifax compromised the security of 143,000,000 households; you need to safeguard the security of every single visitor to your website.

- Your site should be running SSL encryption, particularly if you are gathering ANY customer information (even as little as names and email addresses.)
- The server where your site is hosted should be running frequent and regularly scheduled PCI compliance tests.
- Gather the minimum amount of personal information necessary.

9. DISPOSING OF COMPUTER HARDWARE





DISPOSING OF COMPUTER HARDWARE

- Deleted files are easily recovered, even from a hard drive that has been physically damaged. Deleting files does NOT remove them. Even formatting a drive only makes file recovery more difficult.
- If you are retiring a computer, you should use one of many so-called **disk-wiping or file-shredding utilities** that are available online. These are not for the faint of heart, but the only alternative is to **physically destroy your hard drive** with a hammer and power drill. Here is a link to an updated list: https://www.lifewire.com/free-data-destruction-software-programs-2626174

DISPOSING OF COMPUTER HARDWARE

Did you know that your old copier / fax machine has a hard drive that stores every document that you have ever copied or sent?

Those documents might include your tax returns, employment applications, and other forms with Social Security numbers and other highly secure information.

Be aware of this before disposal!

10. EXERCISE CAUTION. THINK FIRST!

- Always have more than one email account, with one being a recovery account for use when something goes wrong.
- On the other hand, delete any unused (ghost) email accounts, since those only present one more point of potential exploitation.
- Never provide your Social Security number on any website other than the IRS, the Social Security Administration, or your state department of revenue – then be certain that you are at a legitimate site.

EXERCISE CAUTION. THINK FIRST!

- Lock your computers and mobile devices with passwords, PINs, knock codes, or fingerprint or facial recognition software.
- Turn off your computers (or have them go into sleep mode or hibernation) when you leave them.
- Never leave a laptop computer or mobile device unattended, even momentarily.
- Never think it is your “lucky day” and use a USB or flash drive that you find somewhere. It could intentionally contain a virus or malware.

10 STEPS FOR SECURING YOUR DIGITAL IDENTITY

Presented by Peter Pelland, CEO & Founder, Pelland Advertising

Thank you for your attention! Feel free to contact me,
read my columns in Woodall's Campground Management
and other industry publications, and subscribe to my blog.

https://blog.pelland.com
1 800 848-0501
plpelland@pelland.com