Palm Isles Computer Club

Senior Scams

&

Fraud

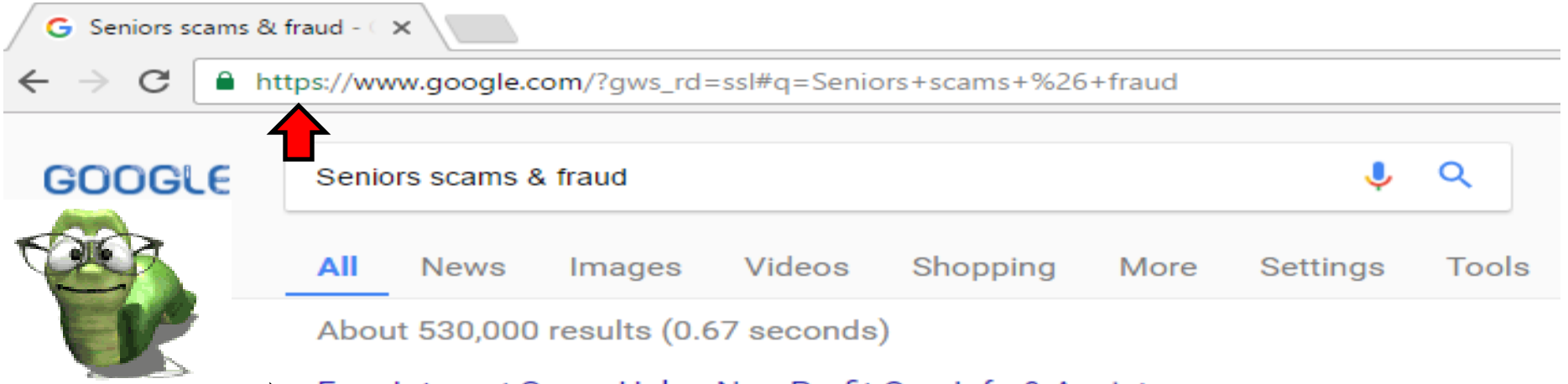
Understanding Fraud and
Our Responsibilities

January 2017

PICC Objectives

Objectives

- What to look for in a web page
- What to click or not click in a web page
- What to lookout for in email
- What to click or not click in email
- What to report and How
- Tips on Safety
- How to Avoid
- Resources of information
- Questions



Google search ….for this will return this many items….
530,000 results (0.67 seconds) information overload.

Don’t let this happen to you!

Protect sensitive personal information

- Look for signs of a secure webpage
- Save financial transactions for home
- Keep sensitive info to yourself
- Avoid scams

Lock shows after click sign-in

Check if Website is Legit

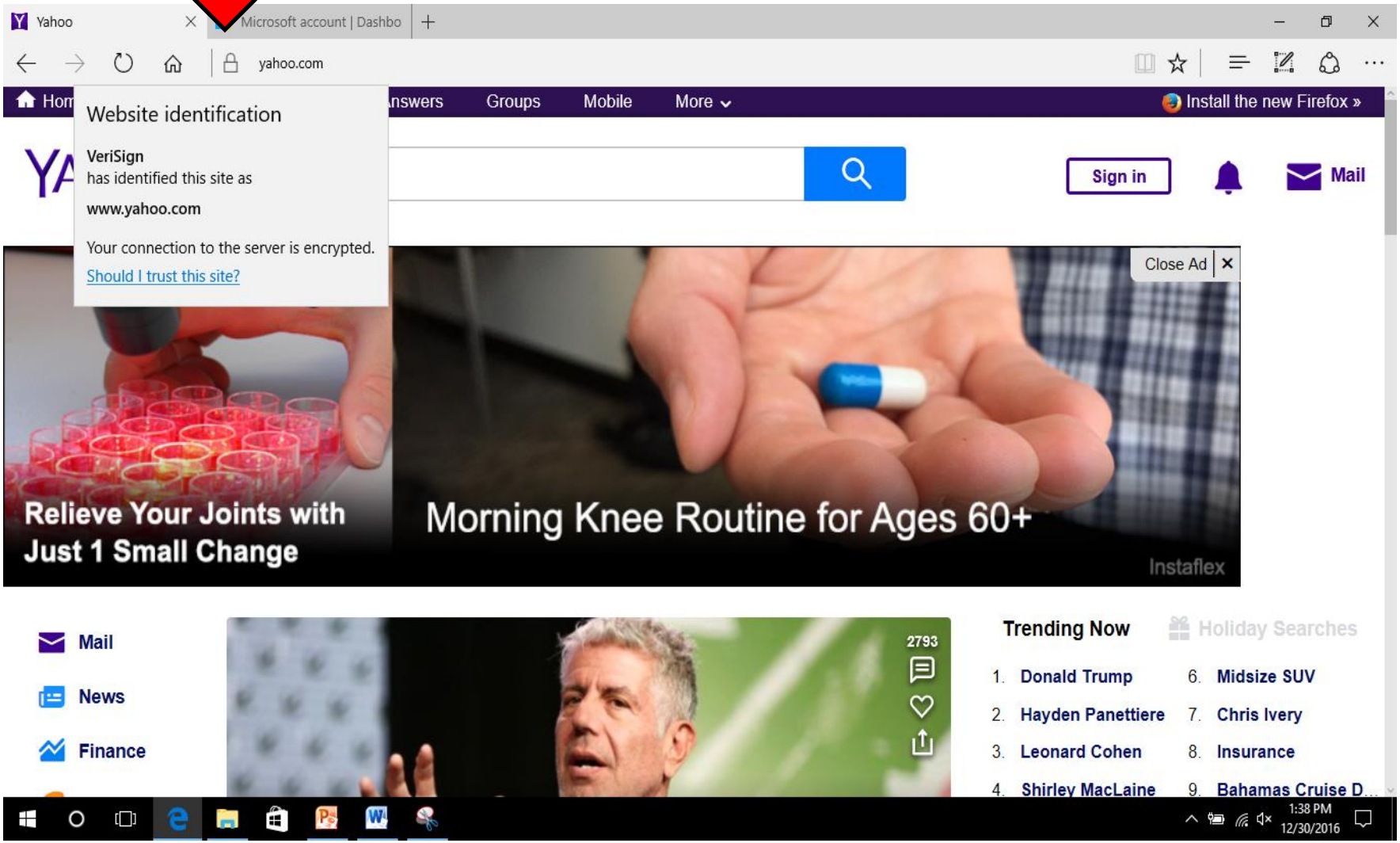
Look at the website address in the address bar of your Internet browser to verify that the website or links you have clicked on did not redirect you elsewhere.

Verify that the website's checkout or payment page is Secure Sockets Layer (SSL) secured to protect your credit card number and other personal information you enter.

SSL secured pages will begin with "https://" instead of "http://"] at the beginning of the web address.

Check the lock Icon

Click the lock icon to check the site.



FBI Cybercrime Division Virus

ICE

The ICE Cyber Crime Center

Your IP-Address: [redacted]
Your Provider: Undefined
Location: United States [redacted]

Your computer has been blocked

The work of your computer has been suspended on the grounds of unauthorized cyber activity.

Possible violations are described below:

Article - 174. Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files). A fine from 18,000 up to 23,000 USD.

Article - 183. Pornography
Imprisonment for the term of up to 2-3 years
(The use or distribution of pornographic files). A fine from 18,000 up to 25,000 USD.

Article - 184. Pornography involving children (under 18 years)
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic files). A fine from 20,000 up to 40,000 USD.

Article - 104. Promoting Terrorism
Imprisonment for the term of up to 25 years without appeal
(Visiting the websites of terrorist groups). A fine from 35,000 up to 45,000 USD with property confiscation.

Article - 68. The distribution of virus programs
Imprisonment for the term of up to 2 years
(The development or distribution of virus programs, which have caused harm to other computers). A fine from 15,000 up to 20,000 USD

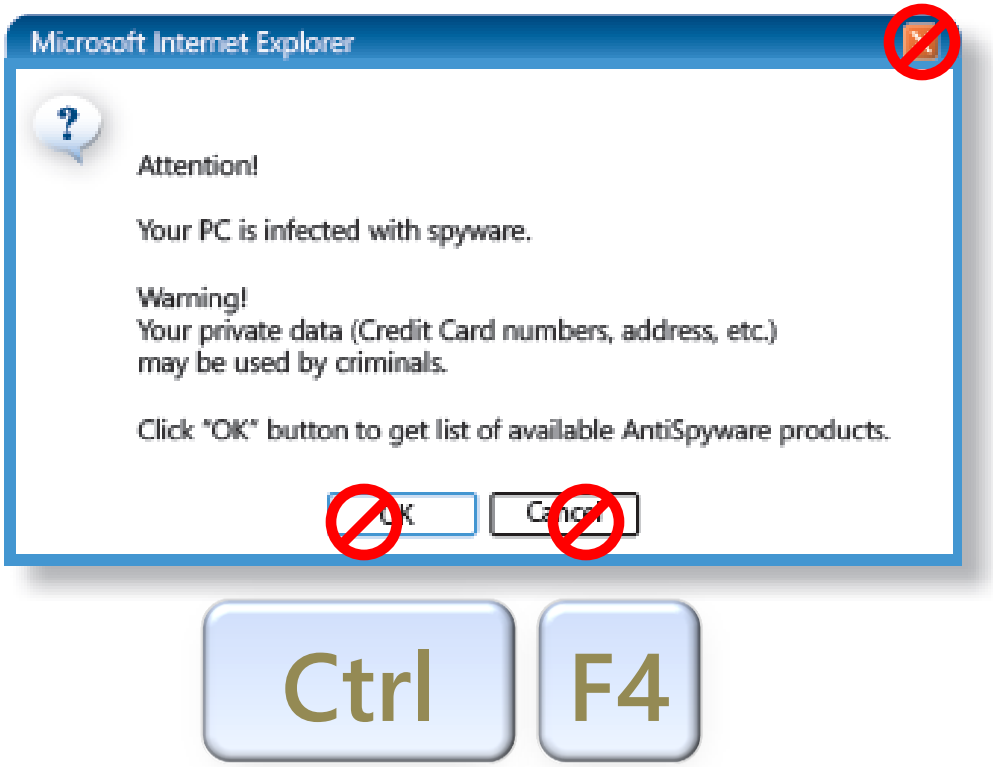
An attempt to unlock the computer by yourself will lead to the full formatting of the operating system. All the files, videos, photos, documents on your computer will be deleted.

All illegal activities conducted through your computer have been recorded in the police database, including photos and videos from your camera for further identification. You have been registered by viewing pornography involving minors.

green dot MoneyPak

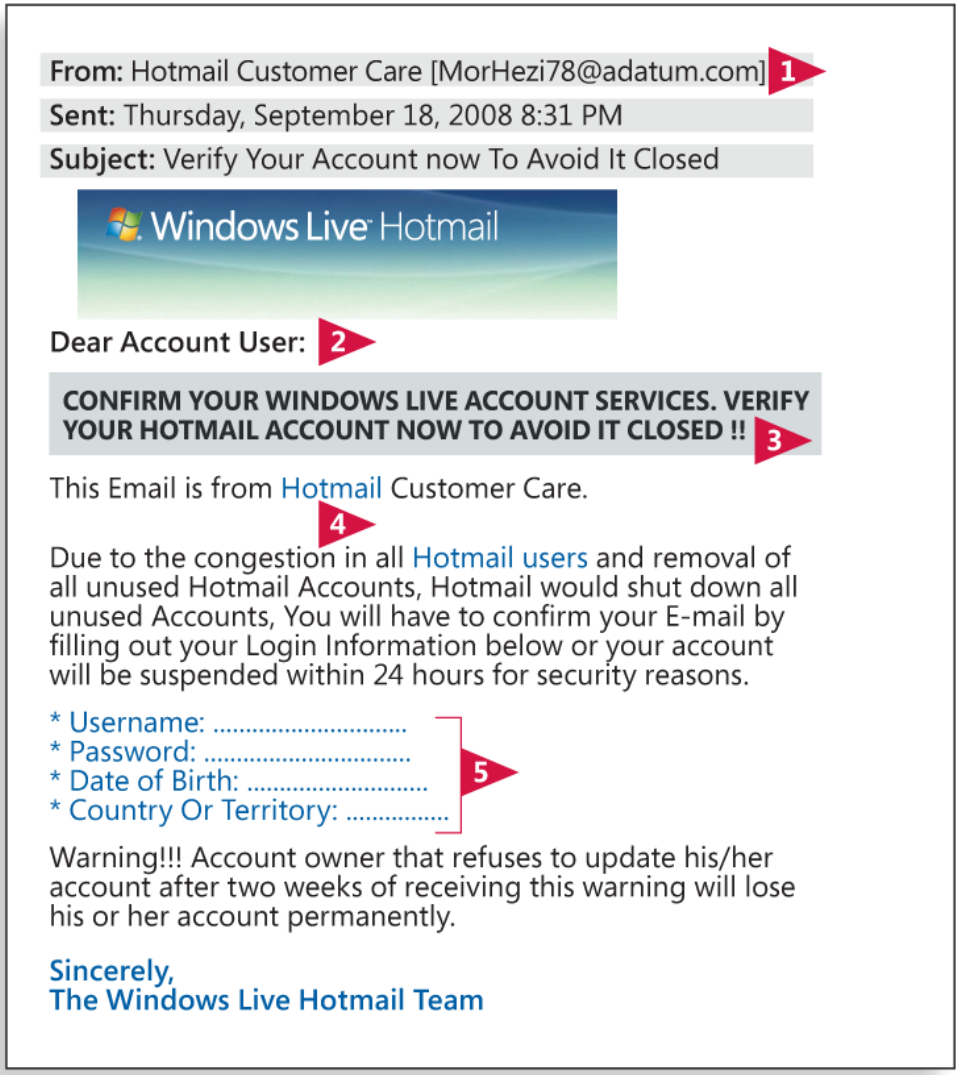
Don’t be tricked into downloading malware

- **Close pop-up messages carefully**



If [Ctrl + F4] does not close the browser then hold down the power button to turn off the computer.

What to look for in Email



From: Hotmail Customer Care [MorHezi78@adatum.com] 1
Sent: Thursday, September 18, 2008 8:31 PM
Subject: Verify Your Account now To Avoid It Closed

Windows Live Hotmail

Dear Account User: 2

CONFIRM YOUR WINDOWS LIVE ACCOUNT SERVICES. VERIFY YOUR HOTMAIL ACCOUNT NOW TO AVOID IT CLOSED !! 3

This Email is from Hotmail Customer Care.

4

Due to the congestion in all Hotmail users and removal of all unused Hotmail Accounts, Hotmail would shut down all unused Accounts, You will have to confirm your E-mail by filling out your Login Information below or your account will be suspended within 24 hours for security reasons.

* Username: .....
* Password: .....
* Date of Birth: .....
* Country Or Territory: .....

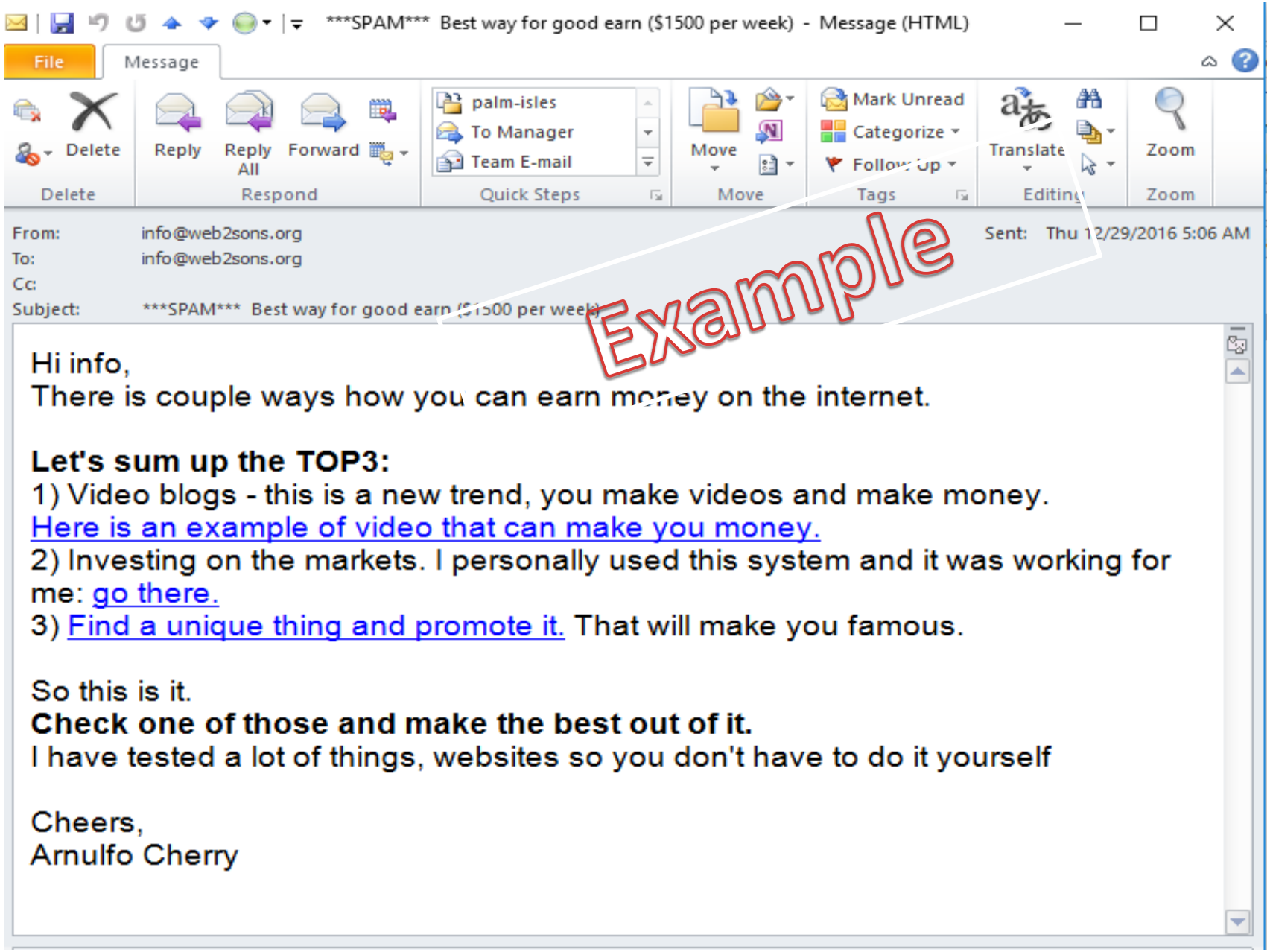
5

Warning!!! Account owner that refuses to update his/her account after two weeks of receiving this warning will lose his or her account permanently.

Sincerely,
The Windows Live Hotmail Team

Learn how to spot scams

1. Suspicious email address
2. Generic salutations
3. Alarmist messages
4. Grammatical errors
5. Requests for personal info


SPAM Best way for good earn ($1500 per week) - Message (HTML)
File
Message
Delete
Reply
Reply All
Forward
palm-isles
To Manager
Team E-mail
Move
Mark Unread
Categorize
Translate
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Zoom
From: info@web2sons.org
To: info@web2sons.org
Cc:
Subject: ***SPAM*** Best way for good earn ($1500 per week)
Sent: Thu 12/29/2016 5:06 AM
Example
Hi info,
There is couple ways how you can earn money on the internet.
Let's sum up the TOP3:
1) Video blogs - this is a new trend, you make videos and make money.
Here is an example of video that can make you money.
2) Investing on the markets. I personally used this system and it was working for me: go there.
3) Find a unique thing and promote it. That will make you famous.
So this is it.
Check one of those and make the best out of it.
I have tested a lot of things, websites so you don't have to do it yourself
Cheers,
Arnulfo Cherry

Phishing

- ✓ **A term is used for emails that claim to be from your bank, a reputable business or a government agency**

- ✓ **Criminals ask for personal information such as Social Security numbers or account numbers to steal funds and/or steal identities**

Fraud & Phishing

Tips

- Most organizations – banks, universities, companies, etc.
  - don't ask for your personal information over email. Beware of requests to update or confirm your personal information.
- Do not open attachments, click links, or respond to email messages from unknown senders or companies.
- Don't access your personal or banking accounts online from a public computer or kiosk.
- Beware of "free" prizes; if you think an offer is too good to be true, then it probably is.
- Make sure you change your passwords often and avoid using the same password for multiple accounts.

Nigerian Letters

- ✓ **E-mails that ask recipients to provide their bank account number to help them share in a big pot of money**
- ✓ **If you respond to these letters you will lose your money**

The Numbers

In 2015, approximately 3.3 million Americans were the victims of technology support scams, suffering a total loss of $1.5 billion. Microsoft is working to spread awareness about how to best protect yourself and your family from digital fraud.

- ✓**According to some estimates, seniors comprise 30 percent of fraud victims**

Top Ten Scams, Schemes, and Frauds

- Home Improvement Fraud
- Debt Relief Fraud
- Funeral Fraud
- Reverse Mortgage Scams
- Investment Scams
- Telemarketing Fraud
- Internet Fraud
- Lottery and Sweepstakes Fraud
- Phony “Government” Scams
- Grandparent Scam

Your Money
Scam Alert

BY SID KIRCHHEIMER

FRAUDS TO WATCH FOR NEXT YEAR

New twists on old con games may snare you

THE YEAR MAY be winding down, but not the ploys that have proved most successful for scammers. Here are the top fraud trends—and what to watch out for in 2017.

PHONE CHEATS

Fraudsters let their fingers do the stalking, especially when targeting older Americans. Crooks will call you, claiming to be tech-support workers who are hunting viruses, utility company bill collectors or even your own grandchildren calling for help from a Mexican jail. In other variations, con artists make pitches for credit cards, extended warranties, and phony sweepstakes and lotteries.

Often they depend on robocalls. The top 40 scam campaigns accounted for the majority of all robocalls this year, reports Pindrop Labs, which tracks telephone fraud.

The newest trend: Identity thieves phone corporate call centers, posing as customers to make illicit bank withdrawals or get loans. Crooks often get names, Social Security numbers and other sensitive data from previous phone scams, explains Ken Shuman, head of global communications at Pindrop.

IRS THREATS

Phone calls from fake IRS agents have netted crooks about $47 million in three years, according to the Treasury Department. The scam will continue next year, but with a twist: The newest likely target will be people with college loans, who are threatened with arrest and other penalties unless a nonexistent "federal student tax" is immediately paid.

Meanwhile, the IRS reported a fourfold surge in tax-related phishing and malware incidents early during this year's filing season. These included the hacking of tax professionals' computers with bogus software updates that allow the criminals access to clients' personal and financial data.

SCARE TACTICS

Like other strong emotions, fear briefly shuts down your brain's logic centers and makes you more likely to react impulsively. In the year ahead, you may encounter frightening but faux threats of arrest, lawsuits and financial ruin for supposedly missing jury duty or not paying a bill.

And some scams are even more frightening: those that include threats of physical harm, such as the "hitman hoax" that seeks payment to cancel a supposed contract on your life, and the "virtual kidnapping" con that often includes background screams and pleas by criminals posing as loved ones who are allegedly being tortured and held for ransom.

A NEW WAY OF PAYOFF

Antifraud groups have raised public awareness that a request for payment by wire transfers and prepaid cash cards usually signals a scam, and the Federal Trade Commission has made it illegal for telemarketers to ask for payment that way. As a result, many scammers have turned to iTunes gift cards as their preferred payment method. In 2017, watch out for come-ons to purchase a card, load money on it and then provide the 16-digit code. It's a fast and virtually untraceable way to steal your money.

Go to **aarp.org/fraudwatchnetwork** to learn more about identity theft and avoiding scams.

Sid Kirchheimer is the author of Scam-Proof Your Life, *published by AARP Books/Sterling.*

AARP Magazine

Phone Cheats

Tech support, bill collectors.

IRS Threats

$47 million in three years.
Hacking Tax Professionals' PCs with bogus software.

Scare Tactics

Fear briefly shuts down brain logic to react impulsively

A New Way of Payoff

Wire Transfers
Prepaid cash cards

Top tips for online safety

1: Defend your devices

Strengthen your devices' defenses - Avoid downloading malware

2: Protect sensitive personal information

Look for signs of a secure webpage (https://) - Save financial transactions for home

Keep sensitive info to yourself

3: Create strong passwords

Use unique, long, and strong passwords & PINs - Keep them secret

4: Take charge of your online reputation

Pay attention to what's online about you - Cultivate an accurate, positive reputation

5: Use social networks more safely

Use Settings or Options to manage your privacy - Accept new friends wisely

Be careful what you post

How To Avoid Internet Fraud

- Avoid filling out forms in emails or on websites that ask for personal information
- Only open attachments from known senders
- Do not click on links in unsolicited emails
- Contact business that supposedly sent the email to verify
- Look for the small yellow lock icon that appears in the browser window
- Do not click on Internet “pop ups”

If you become a victim...

- ✓**Call the police**

  You may need a police report to help you prove that you were a victim

- ✓**Contact your state and local law enforcement agencies such as your district attorney's office or the state attorney general**

Summary

Government Contacts

Federal Trade Commission: www.ftccomplaintassistant.gov

FBI's Internet Crime Complaint Center: www.ic3.gov

Resources

National Council on Aging
https://www.ncoa.org/economic-security/money-management/scams-security/top-10-scams-targeting-seniors/

Identity Theft Resource Center
http://www.idtheftcenter.org/

SCAMS AND SAFETY - FBI
https://www.fbi.gov/scams-and-safety/common-fraud-schemes/seniors

Microsoft tech support scam: www.support.microsoft.com/reportascam

AARP Fraud Watch Network: www.aarp.org/fraudwatchnetwork

Federal Trade Commission: www.ftccomplaintassistant.gov

FBI's Internet Crime Complaint Center: www.ic3.gov

Palm Isles Computer Club

A PDF file is available here: www.web2sons.com