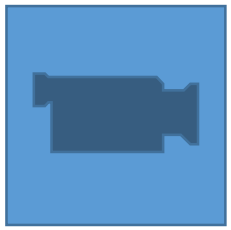
Welcome to our life



DenaliTEK

Cyber Security Awareness Training

What every employee must know about the changing threat landscape of Cyber Crime and what you should do to protect your data

DenaliTEK

Why we're here

- Our experiences with Ransomware and other cyber crimes
- Our mission is "Through teamwork and technology, continually improve every organization we've been given the privilege to serve."

DenaliTEK

Why we're here

- Our experiences with Ransomware and other cyber crimes.
- Our new mission is "Through teamwork and technology, continually protect and improve every organization we've been given the privilege to serve."
- An imperative part of that mission is to bring security focus to the owners and staff who CAN avoid getting breached.

In 2016:
The average time it takes a company to recover from a data breach is 45 days.
The average cost per small business is $38,000.00.

DenaliTEK

Why you're here

- The business' information HAS VALUE to cyber criminals, because YOU need it.
- The business is under attack in many ways.
- You can help prevent an intrusion – you're actually the weakest link!
- It's time to commit to doing your part to protect the business' data

DenaliTEK

Cyber Crime Bonanza on SMB's

- 80% of the breaches in small businesses were preventable
- 60% of the businesses that are breached go out of business in 6 months
- 30% of the victims have fewer than 250 employees

CYBER SECURITY

A New Headline Every Day

DenaliTEK

What Do The Bad Guys Want?

To Steal Information…

- Social Security Numbers
- Credit Numbers
- Bank Account Numbers
- Health Information
- Sales/Donor Lists
- Login Credentials
- Trade Secrets
- Intellectual Property

To Commandeer your PC

- Attack other victims
  (Botnet, DDos)
- Storage
  (Stolen movies, child porn, stolen software)

To Deny You Use of Your Own Info!

- Demand Ransom for Data

DenaliTEK

Cyber Crime is easier than ever

And it's more accessible to everyone

Job postings

Payment systems

Marketplaces

DenaliTEK

How it Works

1. You inadvertently download a file with a spy-agent attached.

2. The agent sits dormant on your PC undetected by Malware/Virus scanning tools

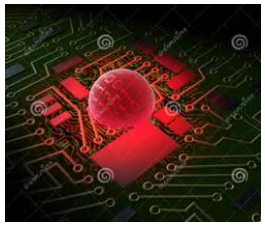
3. The attacker studies the network, undetected, to identify valuable info (trade secrets, credit card numbers, health info) and steals it to sell on the black market.

   ****OR****

   It is added to a collection of other computers housing the same dormant tool into a “basket” with criteria associated, based on your environment.

4. That “basket” is sold (collections run in the thousands) to the highest bidder or for market price, and the buyer is given the code to activate the dormant agent.

5. That buyer then uses the dormant agent to deploy malicious activity.



DenaliTEK

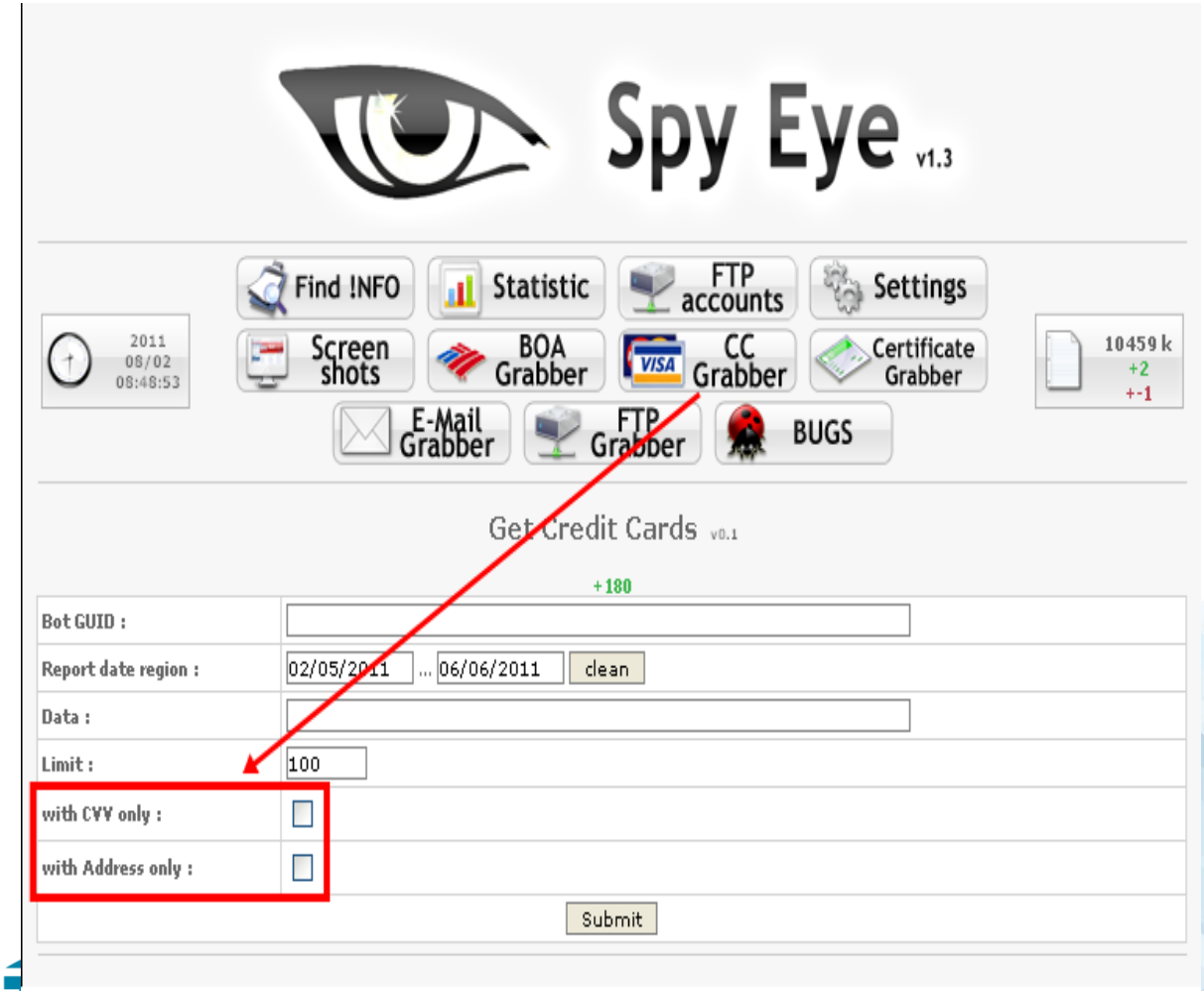
Macs, Mobile Devices-Fair Game

DenaliTEK

Why “work?”

DenaliTEK

Their own online shopping …



DenaliTEK

Cybercriminals know you…

ARE NOT PAYING ATTENTION!

- They study your behavior
- They use you to get around security defenses
- They make you an accomplice to stealing information
- All they need is ONE vulnerable, careless person
- One behavior can cost your business thousands to millions of dollars

DenaliTEK

Entryway #1: Phone Calls

published by KnowBe4

CYBERHEIST NEWS
Arming You With The Facts.

CyberheistNews Vol #6 #03 Jan 19, 2016

Scam Of The Week: Dell Tech Support Service Tag Hack

This is a real one. A number of people using Dell PCs have been contacted by scammers claiming to be Dell Tech Support who actually had specific data that only Dell could have had. We're talking the customer service tag number, a support number printed on a sticker on every Dell computer. I have used Dell machines for 20 years and am very familiar with that sticker.

This is a variant on the Microsoft tech support scam where they call PC users and claim they have detected a problem with the person's computer and need to fix it. End-users gullible enough to give access to their workstations (usually via remote software), are billed hundreds of dollars on their credit card but the scammers of course don't fix anything — and in some cases their PCs are infected with ransomware until they pay up.

DenaliTEK

#2: Social Engineering

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information.

LinkedIn – build a company org chart based on employees & titles. Gather linked vendors to pose as.

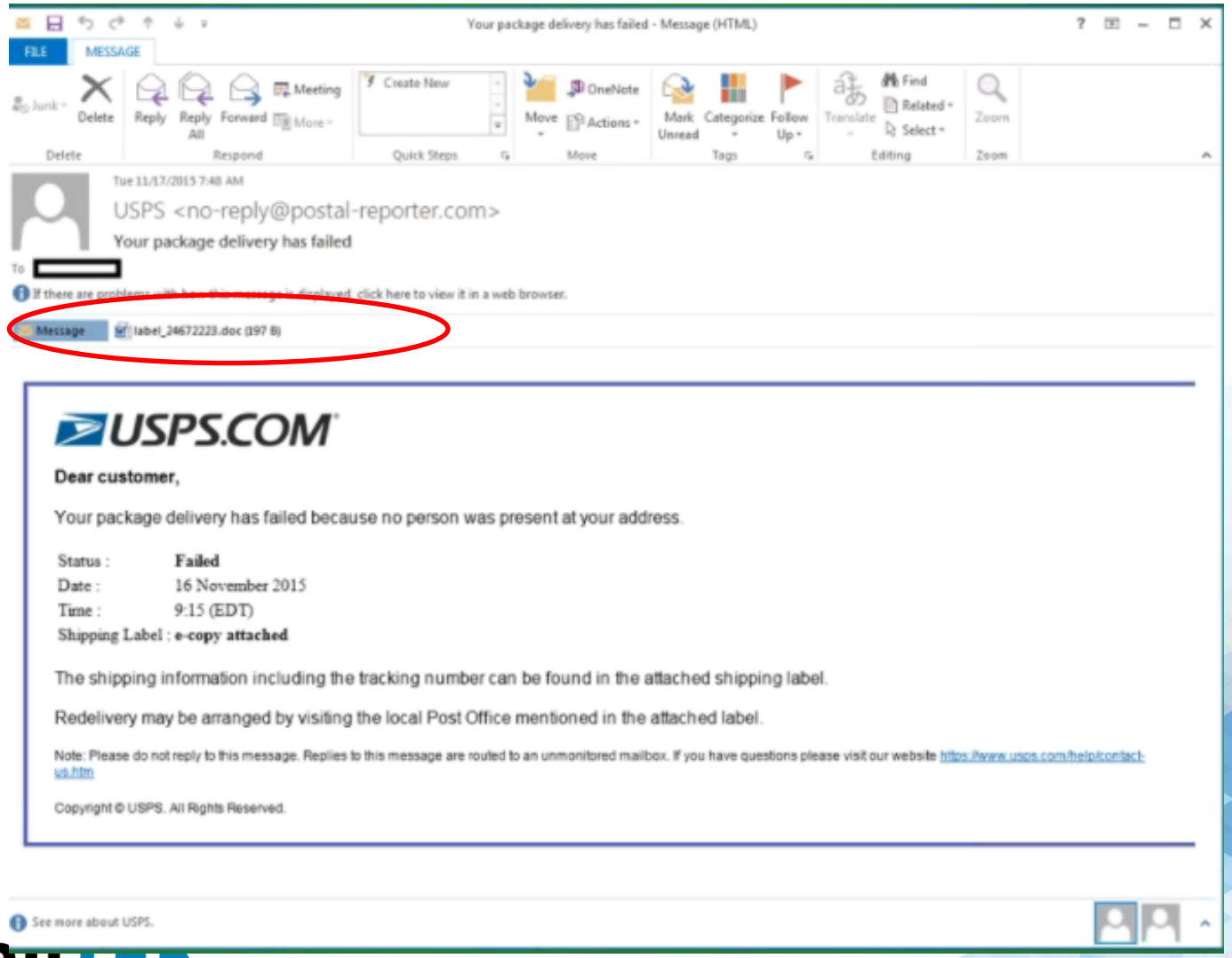
FaceBook – gather employee family members, associations, marital status, birthdates, hobbies, etc for purposes of uncovering passwords

Twitter – get to know your interests, flattery

SnapChat etc – facial recognition and location (who and where you hang out)

DenaliTEK

#3: Phishing Emails



#4: CEO Fraud Emails

Wire Transfer Fraud

"Of the 3rd party involvement claims filed in 2016, half involved phishing and social engineering that led to the fraudulent transfer of money from the victim company to the criminal perpetrators. The cost of these incidents ranged from $26,000 to $400,000, ***all in crisis services***.

We do not believe that these numbers include the amounts of money fraudulently transferred."

~ NetDiligence 2016 Cyber Claims Study; Lloyds of London

DenaliTEK

#5: Infected Websites

Legitimate websites can have malicious ads

Bing Search, Yahoo Search, and LA Times all have been hit with infected ads on their "legitimate" websites

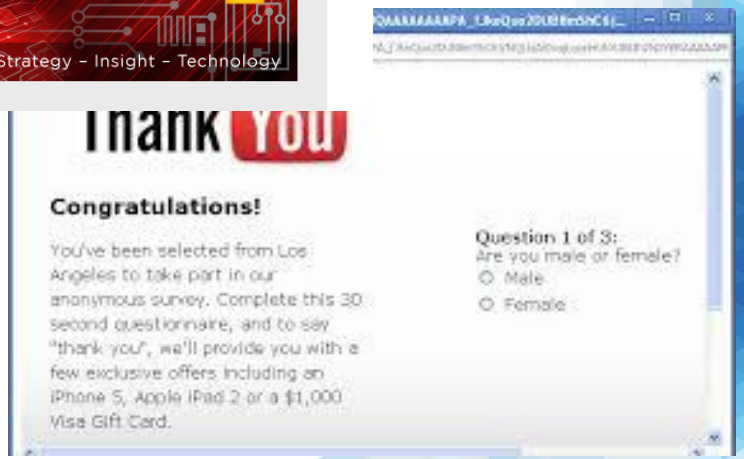
6 SEP 2013 NEWS

L.A. Times, Salon.com Hit By Large-Scale Malvertising Campaign

A wide-scale malvertising campaign targeting the L.A. Times and other name-brand sites has been uncovered

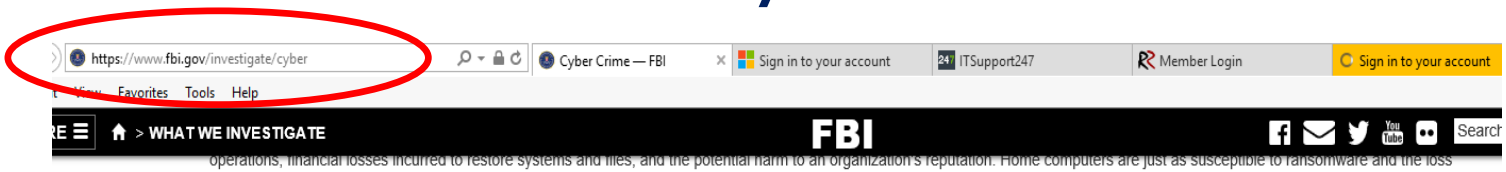
Blue Coat has uncovered a raft of malicious domains sending traffic to the searcherstypedisckruns.com/.net/.org family of Blackhole sites, including adhidclick.com, ortclick.com and several other sibling sites.

This "funnel" layer of the malvertising network was driving so much traffic – tens of thousands of hits – that Chris Larsen, Blue Coat's malware lab architect, looked into where it was all coming from. It turns out that several large, consumer-facing sites were the originators, including the *LA Times*, Salon.com, LA Weekly, the *Fiscal Times*, The Knot Wikia and the ubiquitous ad server site, doubleclick.com.



DenaliTEK

So what can you do?



operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation. Home computers are just as susceptible to ransomware and the loss of access to personal and often irreplaceable items— including family photos, videos, and other data—can be devastating for individuals as well.

In a ransomware attack, victims—upon seeing an e-mail addressed to them—will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax, but which actually contains the malicious ransomware code. Or the e-mail might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software.

One the infection is present, the malware begins encrypting files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network that the victim computer is attached to. Users and organizations are generally not aware they have been infected until they can no longer access their data or until they begin to see computer messages advising them of the attack and demands for a ransom payment in exchange for a decryption key. These messages include instructions on how to pay the ransom, usually with bitcoins because of the anonymity this virtual currency provides.

Ransomware attacks are not only proliferating, they're becoming more sophisticated. Several years ago, ransomware was normally delivered through spam e-mails, but because e-mail systems got better at filtering out spam, cyber criminals turned to spear phishing e-mails targeting specific individuals. And in newer instances of ransomware, some cyber criminals aren't using e-mails at all—they can bypass the need for an individual to click on a link by seeding legitimate websites with malicious code, taking advantage of unpatched software on end-user computers.

The FBI doesn't support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee an organization that it will get its data back—there have been cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals.

So what does the FBI recommend? As ransomware techniques and malware continue to evolve—and because it's difficult to detect a ransomware compromise before it's too late—organizations in particular should focus on two main areas:

- Prevention efforts—both in both in terms of awareness training for employees and robust technical prevention controls; and
- The creation of a solid business continuity plan in the event of a ransomware attack.

Tips for Dealing with Ransomware. While the below tips are primarily aimed at organizations and their employees, some are also applicable to individual users.

- Make sure employees are aware of ransomware and of their critical roles in protecting the organization's data.
- Patch operating system, software, and firmware on digital devices (which may be made easier through a centralized patch management system).
- Ensure antivirus and anti-malware solutions are set to automatically update and conduct regular scans.
- Manage the use of privileged accounts—no users should be assigned administrative access unless absolutely needed, and only use administrator accounts when necessary.
- Configure access controls, including file, directory, and network share permissions appropriately. If users only need read specific information, they don't need write-access to those files or directories.
- Disable macro scripts from office files transmitted over e-mail.
- Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations (e.g., temporary folders supporting popular Internet browsers, compression/decompression programs).
- Back up data regularly and verify the integrity of those backups regularly.
- Secure your backups. Make sure they aren't connected to the computers and networks they are backing up.

De

Let's start with passwords

39% **Percentage of adults in the U.S. using the same or very similar passwords for multiple online services, which increases to 47% for adults age 18-29**

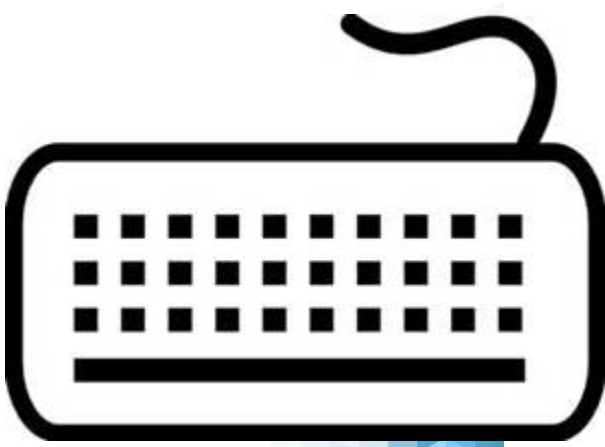
Passwords are a twentieth-century solution to a twenty-first century problem. Unfortunately, user names and passwords - the most common digital credentials used today - are all that stands between your employees and vital online services including corporate networks, social media sites, e-commerce sites and others. A good security practice is to use a completely different password for every service, but the fact is that nearly 40% of Americans replicate the same or very similar passwords for each service they use.

Pew Research Center, "Americans and Cybersecurity", January 2017

DenaliTEK

IT Security Suggestions

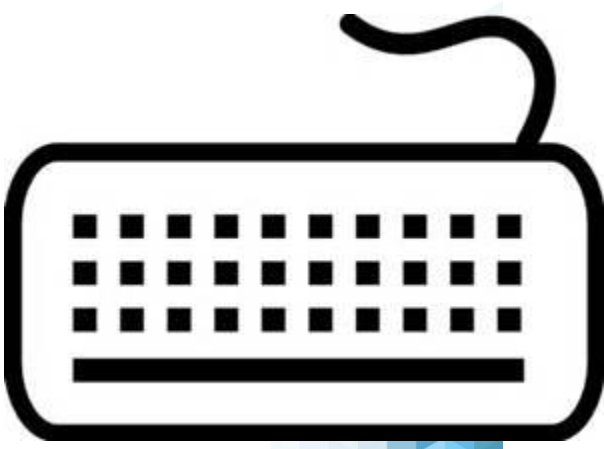
- **Passwords**
  - Strong passwords that rotate every six months
    Example 1:
    - Animal (static)
      Antelope
    - 2nd Character cap
      aNtelope
    - How many letters total?
      aNtelope8
    - How many vowels? aNtelope84
    - One character or symbol
      aNtelope84/
  - Example 2:
    - Phrase: Crazy Hackers Can't Guess My Password
      1510 chcgmP1510*



DenaliTEK

IT Security Suggestions

- **Passwords**
  - AVOID!
    - Words (happy, library, milk)
    - No spouse, kids, parents, or pet's names
    - Don't use any phone number or portion of
    - Birthdates – yours, kids, spouse, parents
    - Business topic or category you are in (i.e. charity or cooking)
    - Never change only last 2 characters when updating (password12; password 13; etc)
    - Never reverse spelling of a word



DenaliTEK

Understanding domains

Understand the domain name significance – what follows the period is the extension

- **.com – least safe**
- **.org and .net – 2nd least safe**
- **.edu – pretty safe; it's an educational institution**
- **.gov – very safe generally**

What precedes it is the name of the domain.

Difference between:

http://www.support.la-itgirl.com and http://www.support.laitgirl.com

Difference between http://www.ford.buyerrights.com and http://www.ford.com/buyerrights

DenaliTEK

Identify the correct domain

Understand the domain name significance

- **.com – least safe**
- **.org and .net – 2nd least safe**
- **.edu – pretty safe; it's an educational institution**
- **.gov – very safe generally**

Difference between:
http://www.support.la-itgirl.com and
http://www.support.laitgirl.com

Difference between
http://www.ford.buyerrights.com and
http://www.ford.com/buyerrights

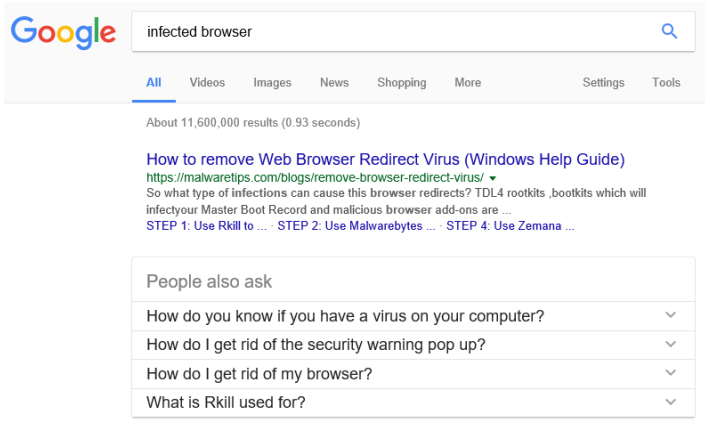
DenaliTEK

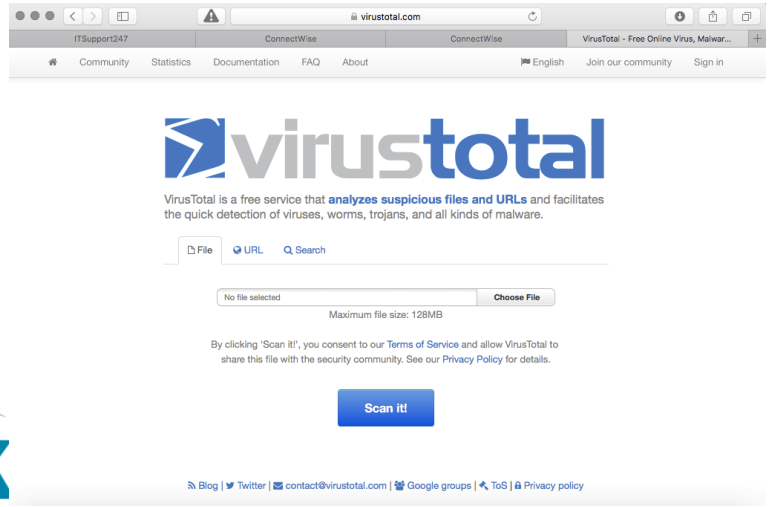
Safe web searches

Web Search sample:

- **Note the actual URL that you are being sent to**
  - **Ignore Blue Header**
  - **Read full URL of green or http: address**
  - **Unsure?** https://virustotal.com to check if you're unsure!

WHICH OF THESE SEARCH RESULTS WOULD YOU OPEN?

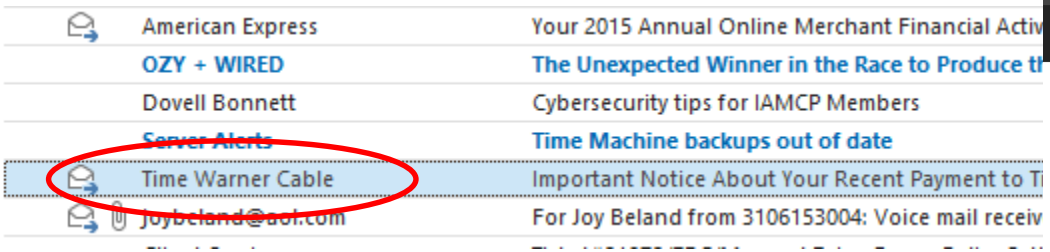


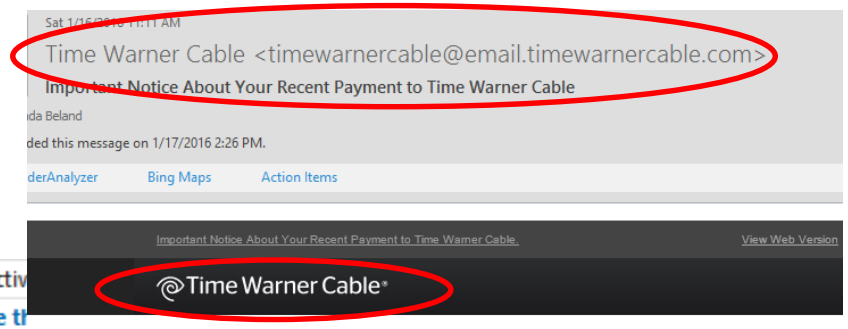


DenaliTEK

Scrutinize email

- **What you can do - Email:**
  - Which of these emails would you be very careful opening?



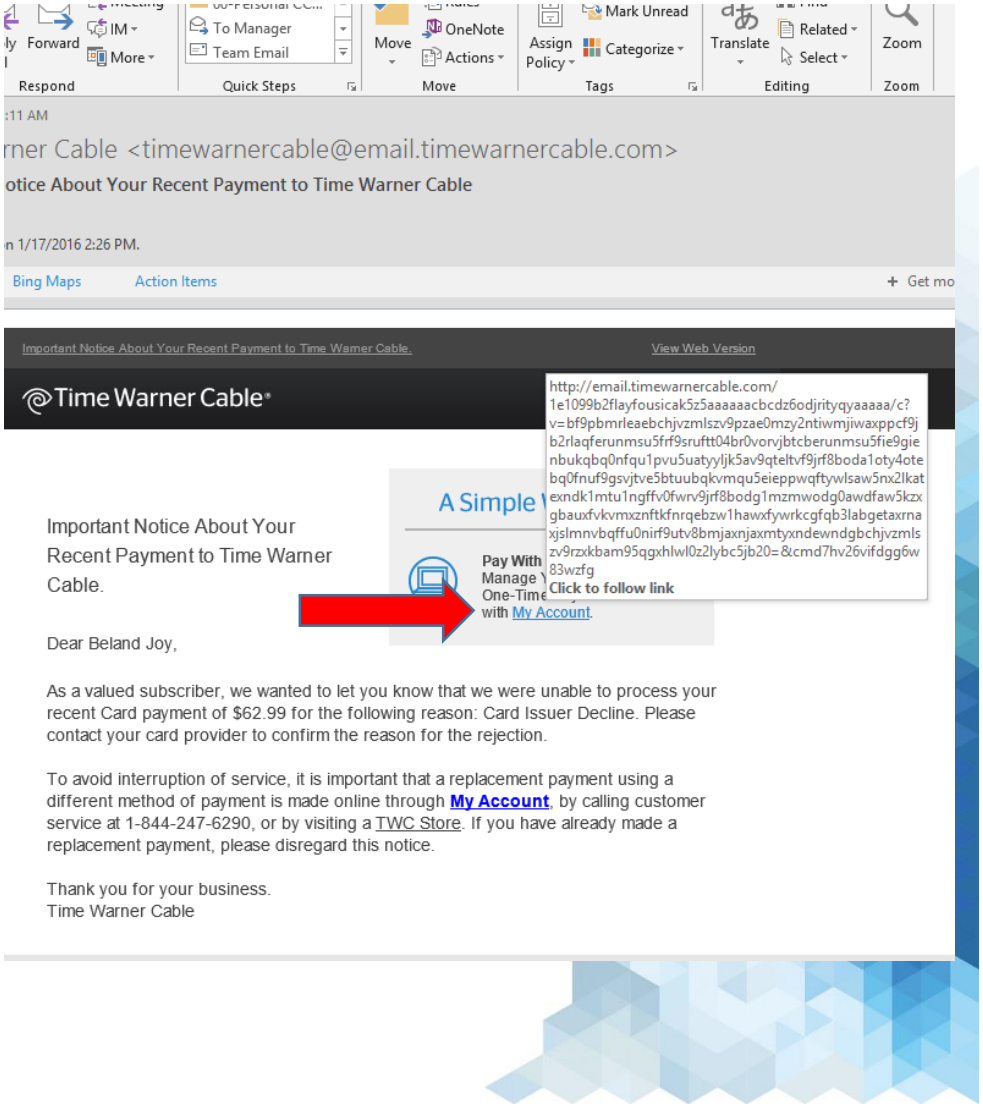


  - What areas can you check to see if it's valid?
    - Sender actual email address
    - Logos
    - URL's to click on

DenaliTEK

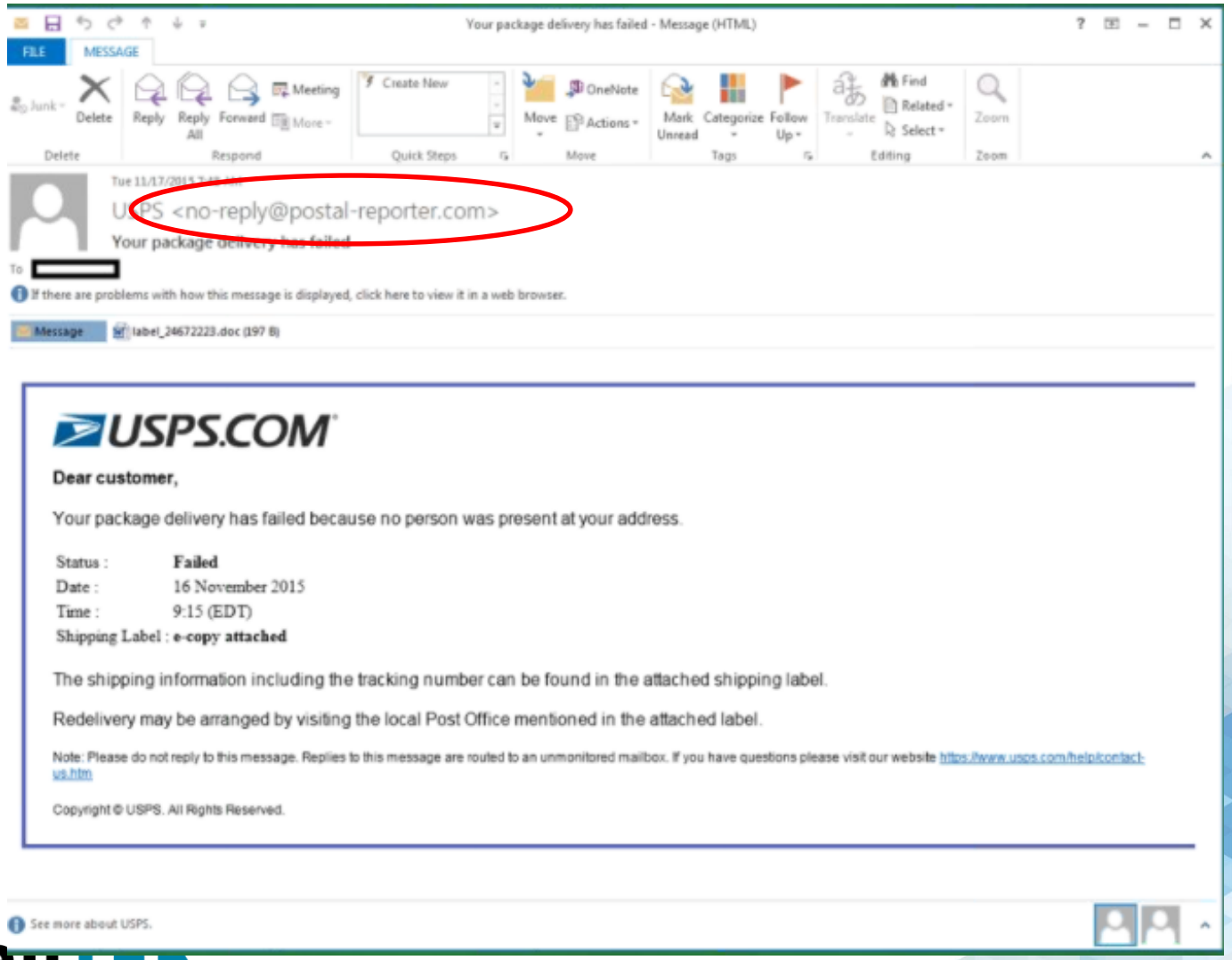
Look before you click

- **The URL "hover":**
  - **Be the master of your mouse universe.**



DenaliTEK

They are CONVINCING



And protect the data!

- **Data storage:**
  - **Lock your PC when away from your desk (5 min)**
  - **No personal USB drives**
  - **No personal Google, DropBox or OneDrive accounts used for business or on business computers**
  - **Don’t email business work to your personal email account. Litigation concerns for personal accounts**
  - **Stick with only IT-approved applications**

DenaliTEK

Incident Response

Signs of infection:

- Browser redirecting to a different website than what you'd expect
- New toolbars in the browser or applications on the desktop
- Popups that tell you your computer is infected or that you need to run a tool that you're not expecting and familiar with
- Your computer slows wayyyyyyy dowwwwwwwwwwn
- An overload of coupons or junk mail

- First step: **Unplug the computer from the internet** / network connection (demo blue cables on back of computers). If you're on wi-fi, shut the computer down and do not restart it.
- Second step: **Take a photo of the pop-up or website redirect** with your smart phone and text it to us. Open a service ticket and ask us to call your cell with one of our cells so that you can text it for our review.

DenaliTEK

A minute on privacy

- **What you can do – Mobile Devices**
  - **All Mobile Devices should have a PIN (phones and tablets)**
  - **Turn on Apple iCloud/Find my iPhone, Review all settings (live exercise)**
    - **Settings /Privacy**
      - **/Contacts, Camera**
      - **/Bluetooth Sharing**
      - **/Advertising**
    - **Settings /Privacy /Location Services /Look at list to see what is using your location**
      - **System Services /**
        - **Location-Based iAds**
        - **Frequent Locations**
  - **Back up regularly using iTunes**
  - **Don't download any app that you don't NEED if it's not from an established company**
  - **If you lose it, let us know RIGHT AWAY**

DenaliTEK

And a minute on your homes

http://www.wsj.com/articles/rare | WSJ New Year Sale | Rarely Patche... | Bing | Sagacious | Defi... | Umbrella > Login

DOW JONES, A NEWS CORP COMPANY

DJIA ▲ 16145.66 0.99% Nasdaq ▲ 4529.54 0.92% U.S. 10 Yr ▼ -5/32 Yield 2.055% Crude Oil ▼ 28.90 -1.77% Euro ▲ 1.0900 0.06%

THE WALL STREET JOURNAL.

Subscribe Now | Sign In

JANUARY SALE. 50% OFF.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

Rarely Patched Bugs in Home Wi-Fi Hookups Cripple Security

Apple, Alphabet, Yahoo Hoping to Use Super Bowl to Score at Home

WhatsApp to Drop Subscription Fee

583

TECH

Rarely Patched Software Bugs in Home Routers Cripple Security

Wi-Fi devices, vulnerable to hackers, show difficulty of updating software after release

By JENNIFER VALENTINO-DEVRIES

Jan. 18, 2016 11:58 a.m. ET

In late 2014, a small Massachusetts software company got an ominous email: A computer-security researcher said a flaw in one of its programs put millions world-wide at risk of being hacked.

Engineers at the company, Allegro Software Development Corp., analyzed the flaw in the program, which can help users access the controls of home Internet routers. They quickly realized something strange: They had fixed this bug nearly 10 years...

DenaliTEK

Partner with your IT Support

Policies and procedures are there to protect you and the business.

You don't want to be "That guy."

DenaliTEK

We will follow up with an email full of resources and three quick questions about this training.

Please refer us!
Stay safe out there.

DenaliTEK