Stew Jensen

nxtConcepts

VP / Partner

A forward thinking, non-traditional agency

creative thinkers | brand enhancers | strategic planners

results obsessed | rule breakers

nxtconcepts

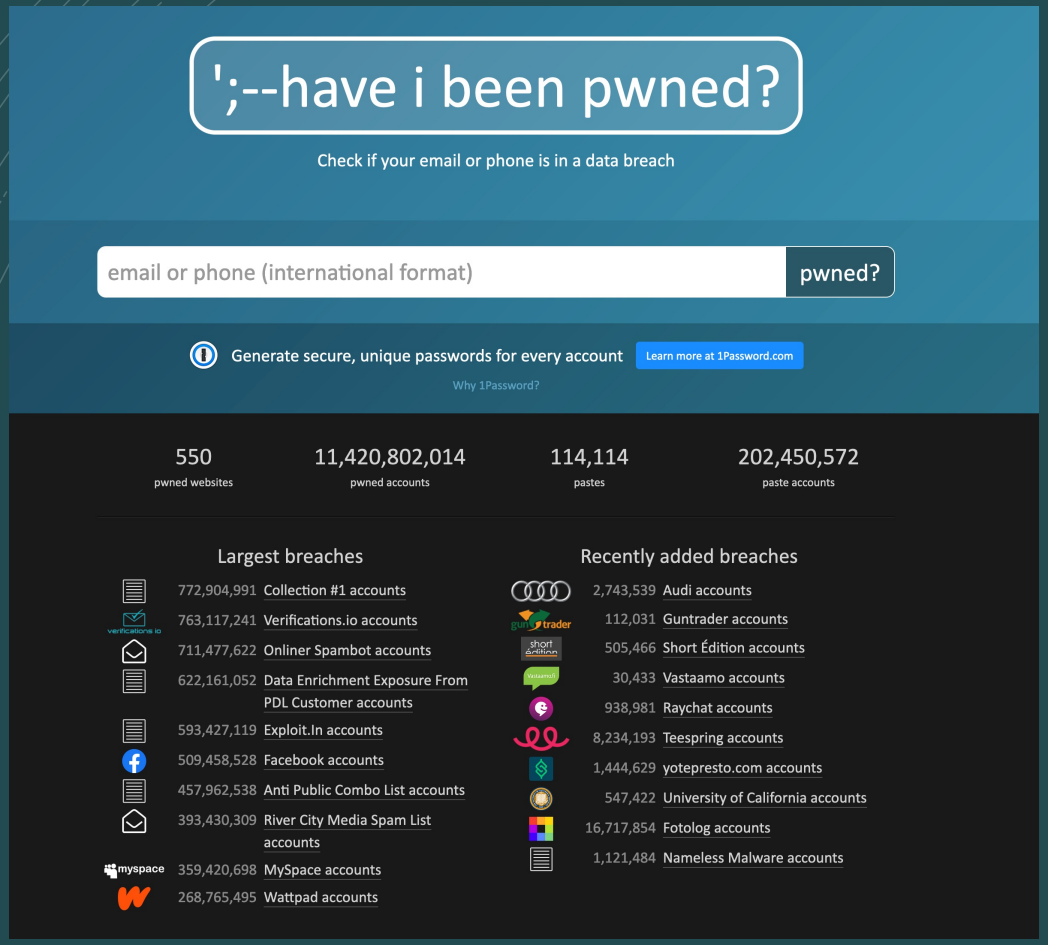
Cybersecurity is Harder than Snowmaking.

Are you Prepared?

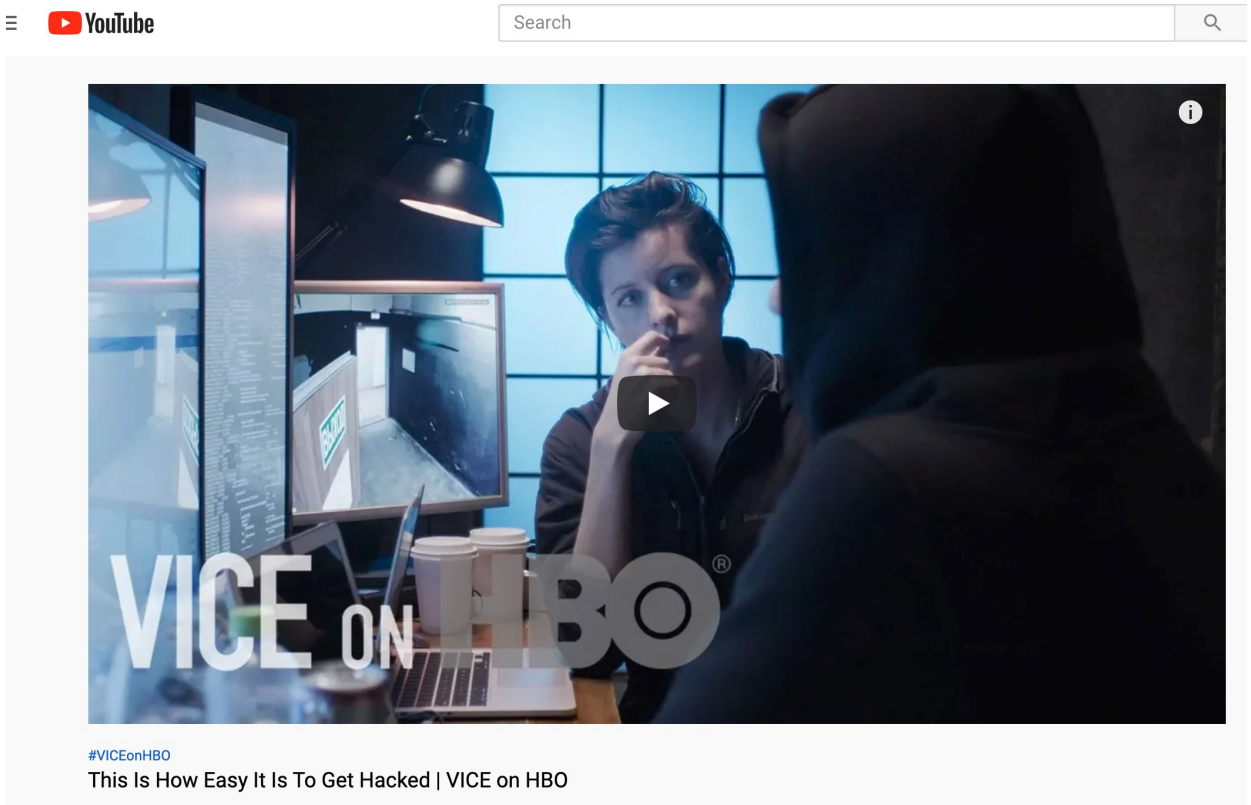
Topics

-How bad is it?
-Anatomy of a Ransomware Attack
-Why You Will Be Hacked
-Pay or Don’t Pay
-What to do today
-What to do tomorrow

How many people here have been a victim to cybercrime?


';--have i been pwned?
Check if your email or phone is in a data breach
email or phone (international format)
pwned?
Generate secure, unique passwords for every account
Learn more at 1Password.com
Why 1Password?
550
pwned websites
11,420,802,014
pwned accounts
114,114
pastes
202,450,572
paste accounts
Largest breaches
772,904,991 Collection #1 accounts
763,117,241 Verifications.io accounts
711,477,622 Onliner Spambot accounts
622,161,052 Data Enrichment Exposure From PDL Customer accounts
593,427,119 Exploit.In accounts
509,458,528 Facebook accounts
457,962,538 Anti Public Combo List accounts
393,430,309 River City Media Spam List accounts
359,420,698 MySpace accounts
268,765,495 Wattpad accounts
Recently added breaches
2,743,539 Audi accounts
112,031 Guntrader accounts
505,466 Short Édition accounts
30,433 Vastaamo accounts
938,981 Raychat accounts
8,234,193 Teespring accounts
1,444,629 yotepresto.com accounts
547,422 University of California accounts
16,717,854 Fotolog accounts
1,121,484 Nameless Malware accounts

It can happen to anyone

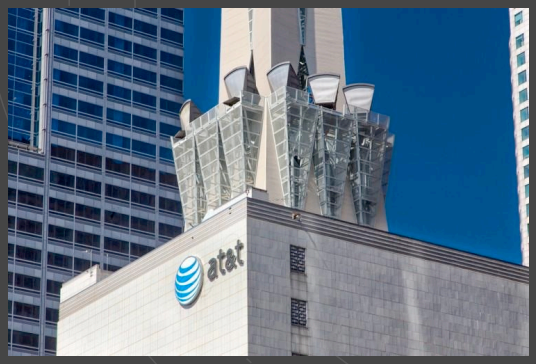


https://www.youtube.com/watch?v=G2_5rPbUDNA

From Big Business

TOYOTA

amazon amazon



To Small

The National Cyber Security Alliance has recently released statistics that show 20% of small businesses experience such an attack every year, and that 60% of these businesses were forced to close within 6 months of being hacked.

Data Security by CimTrak. PHOTO: Cybercrime Magazine.

60 Percent Of Small Companies Close Within 6 Months Of Being Hacked

To Nuclear

THE KANSAS CITY STAR.

LOCAL

Russia infiltrated Kansas nuclear plant's business network, FBI and DHS say

BY MAX LONDBERG

MARCH 16, 2018 06:51 PM, UPDATED MARCH 18, 2018 12:49 PM

Wolf Creek Nuclear power plant in Burlington, Kan. FILE PHOTO *ASSOCIATED PRESS*

To Airports

62° Albany

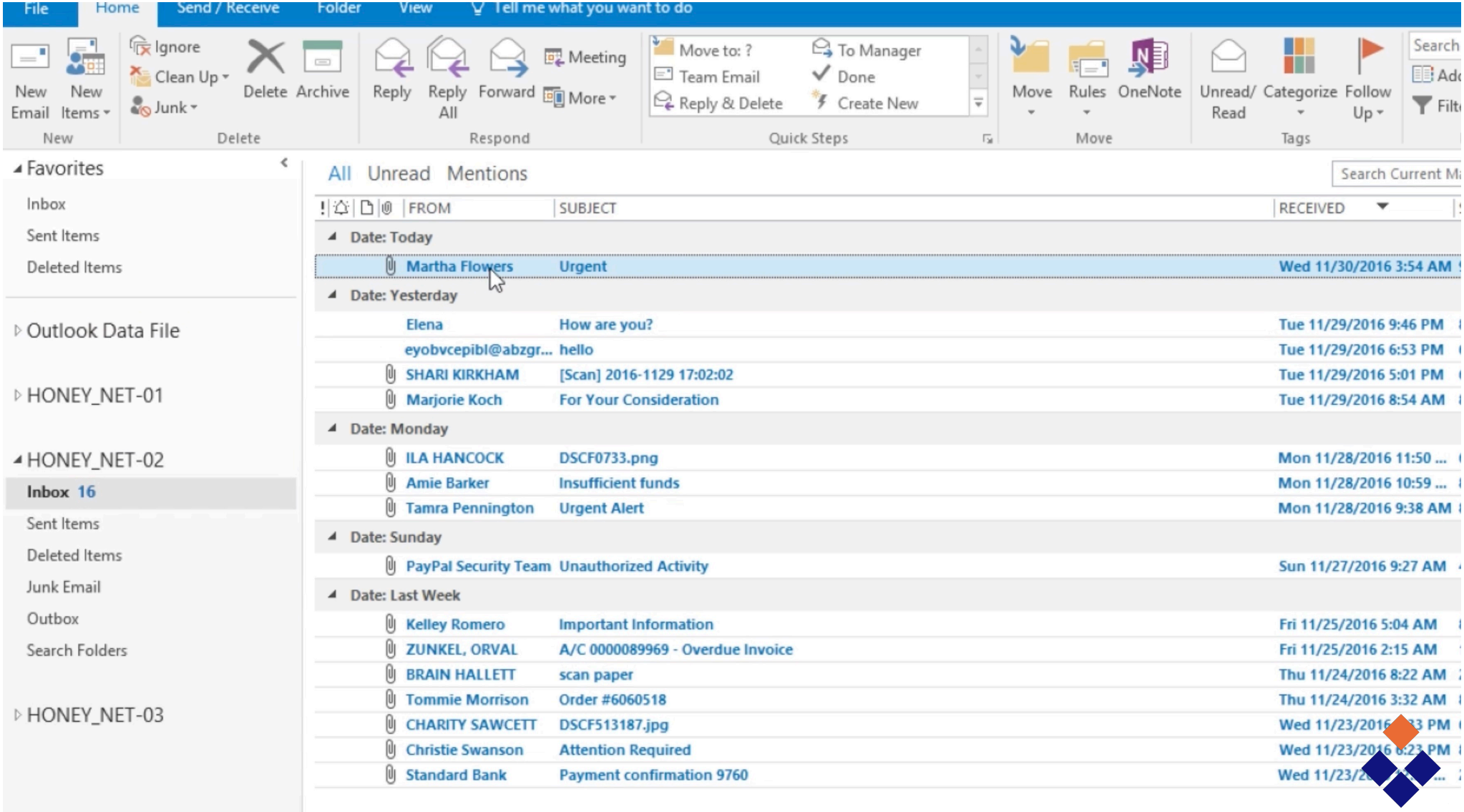
YOUR LOCAL NEWS LEADER

NEWS ALBANY NY WEATHER TRAFFIC WATCH LIVE NEWS SPORTS JOBS 10 IN TOGA COM

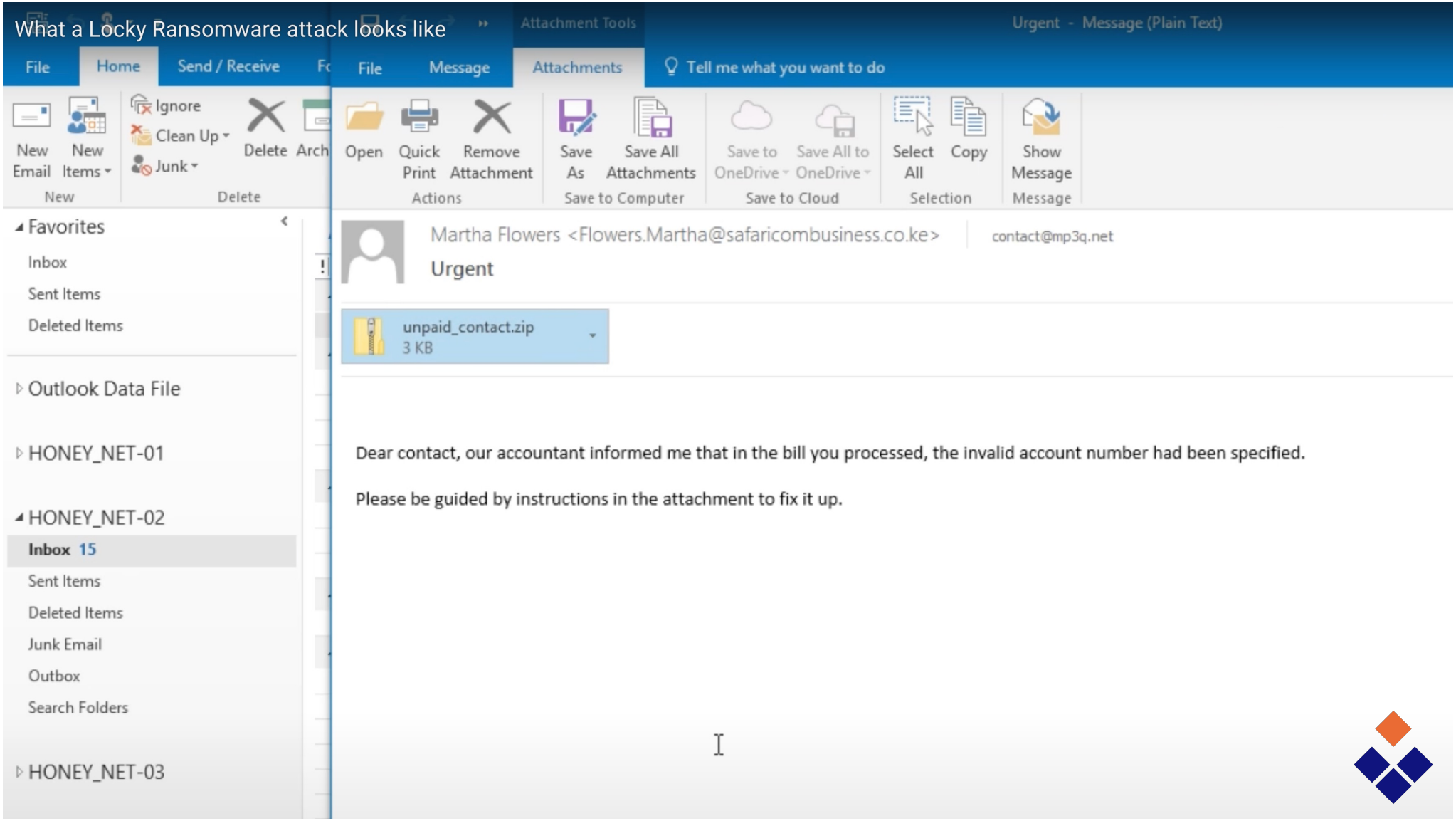
LOCAL

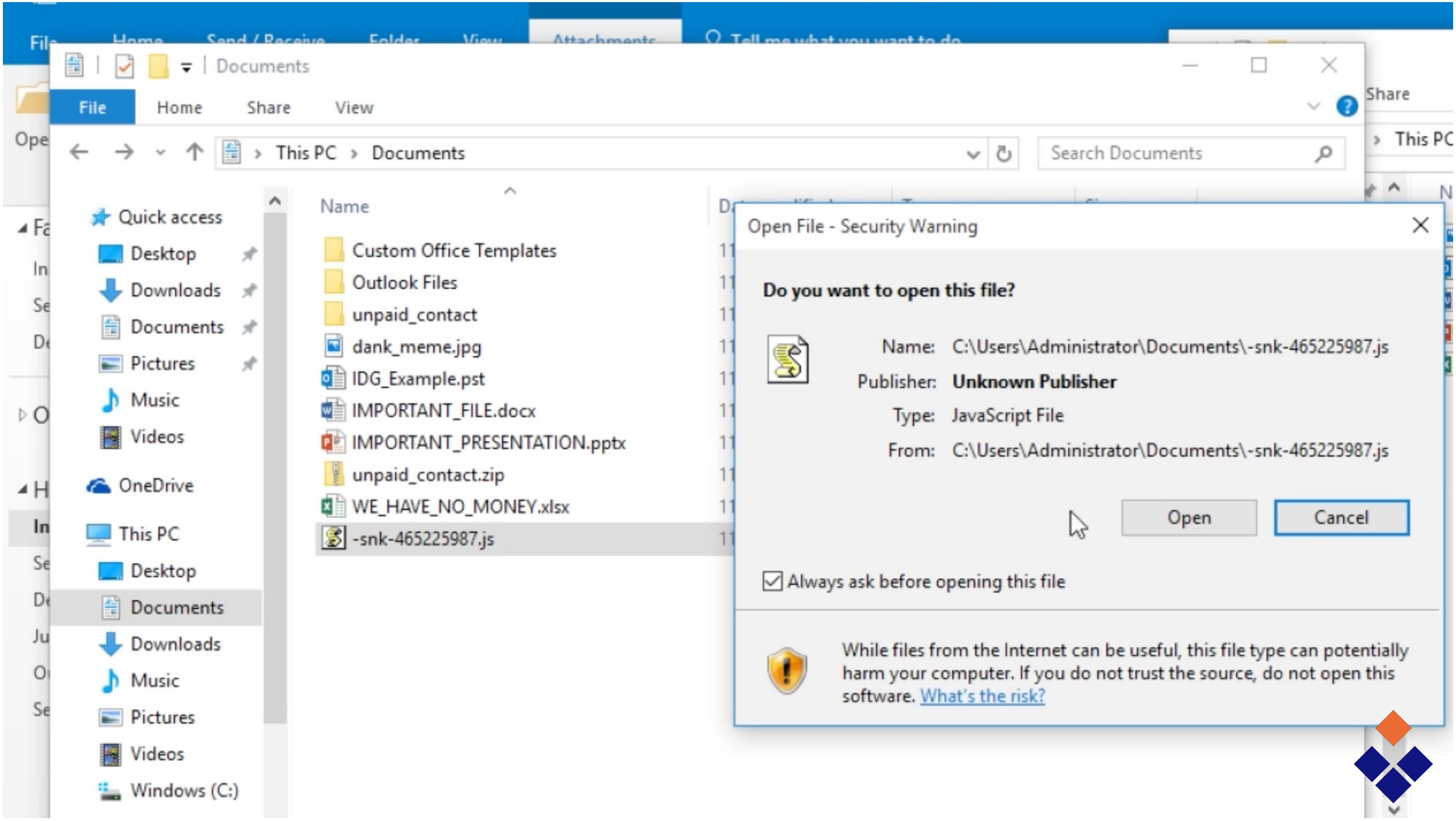
Albany airport pays ransom after hit by cyber hackers

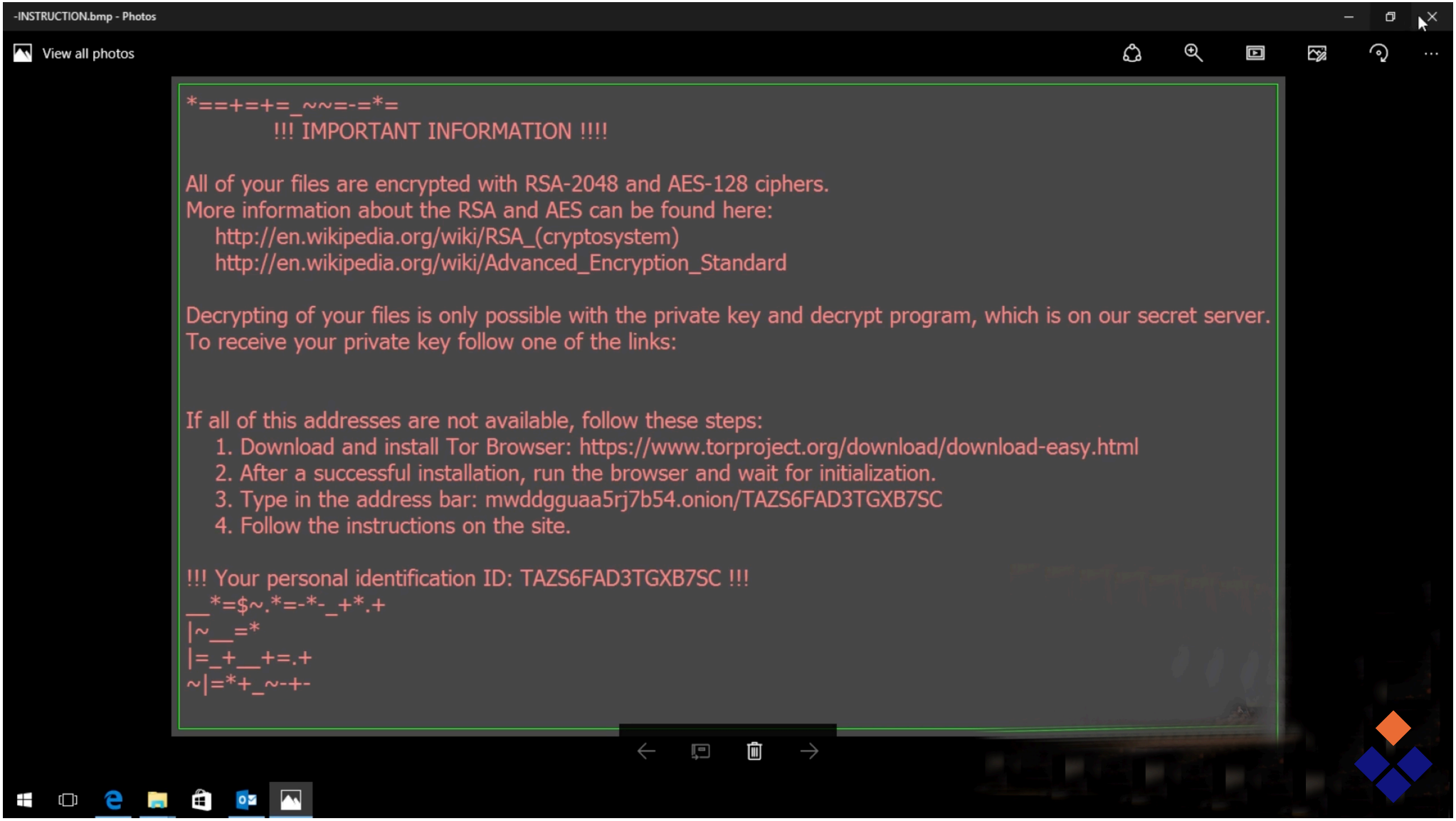
The Anatomy of a Ransomware Attack

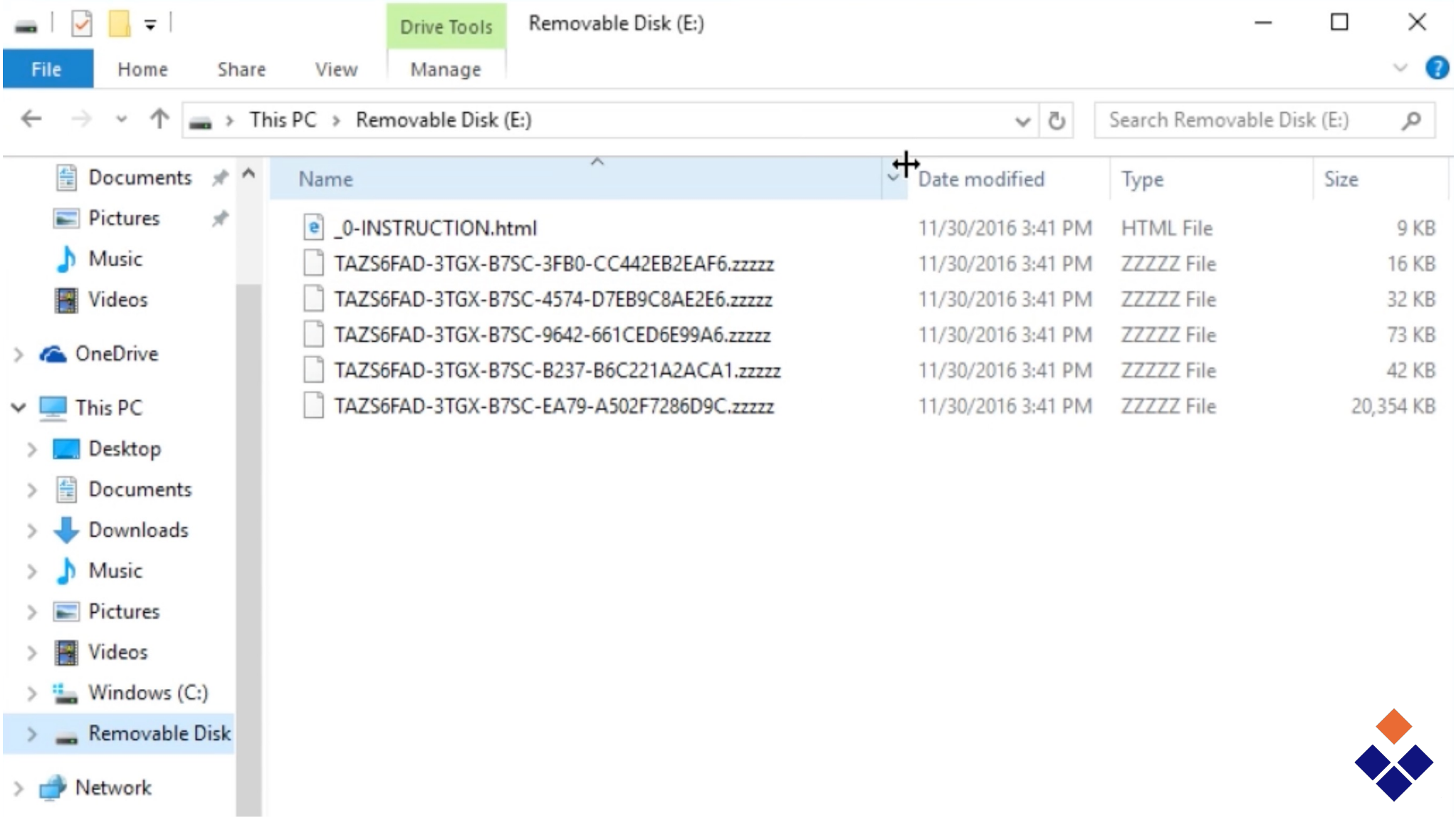

File
Home
Send / Receive
Folder
View
Tell me what you want to do
New Email
New Items
Ignore
Clean Up
Junk
Delete
Archive
Reply
Reply All
Forward
Meeting
More
Move to: ?
Team Email
Reply & Delete
To Manager
Done
Create New
Move
Rules
OneNote
Unread/ Read
Categorize
Follow Up
New
Delete
Respond
Quick Steps
Move
Tags
Favorites
Inbox
Sent Items
Deleted Items
Outlook Data File
HONEY_NET-01
HONEY_NET-02
Inbox 16
Sent Items
Deleted Items
Junk Email
Outbox
Search Folders
HONEY_NET-03
All
Unread
Mentions
Search Current Ma
FROM
SUBJECT
RECEIVED
Date: Today
Martha Flowers
Urgent
Wed 11/30/2016 3:54 AM
Date: Yesterday
Elena
How are you?
Tue 11/29/2016 9:46 PM
eyobvcepibl@abzgr...
hello
Tue 11/29/2016 6:53 PM
SHARI KIRKHAM
[Scan] 2016-1129 17:02:02
Tue 11/29/2016 5:01 PM
Marjorie Koch
For Your Consideration
Tue 11/29/2016 8:54 AM
Date: Monday
ILA HANCOCK
DSCF0733.png
Mon 11/28/2016 11:50 ...
Amie Barker
Insufficient funds
Mon 11/28/2016 10:59 ...
Tamra Pennington
Urgent Alert
Mon 11/28/2016 9:38 AM
Date: Sunday
PayPal Security Team
Unauthorized Activity
Sun 11/27/2016 9:27 AM
Date: Last Week
Kelley Romero
Important Information
Fri 11/25/2016 5:04 AM
ZUNKEL, ORVAL
A/C 0000089969 - Overdue Invoice
Fri 11/25/2016 2:15 AM
BRAIN HALLETT
scan paper
Thu 11/24/2016 8:22 AM
Tommie Morrison
Order #6060518
Thu 11/24/2016 3:32 AM
CHARITY SAWCETT
DSCF513187.jpg
Christie Swanson
Attention Required
Standard Bank
Payment confirmation 9760

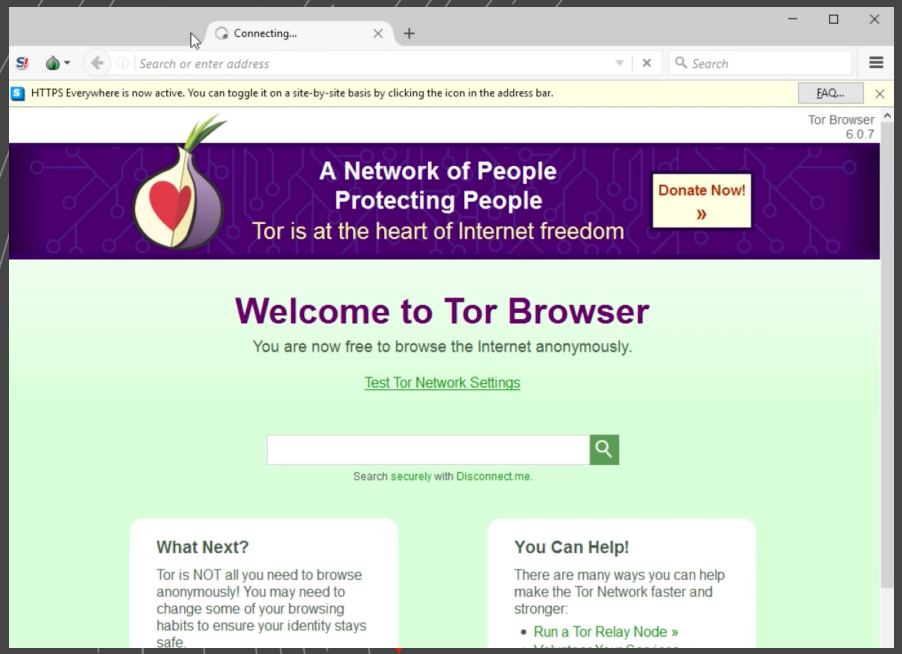
What a Locky Ransomware attack looks like

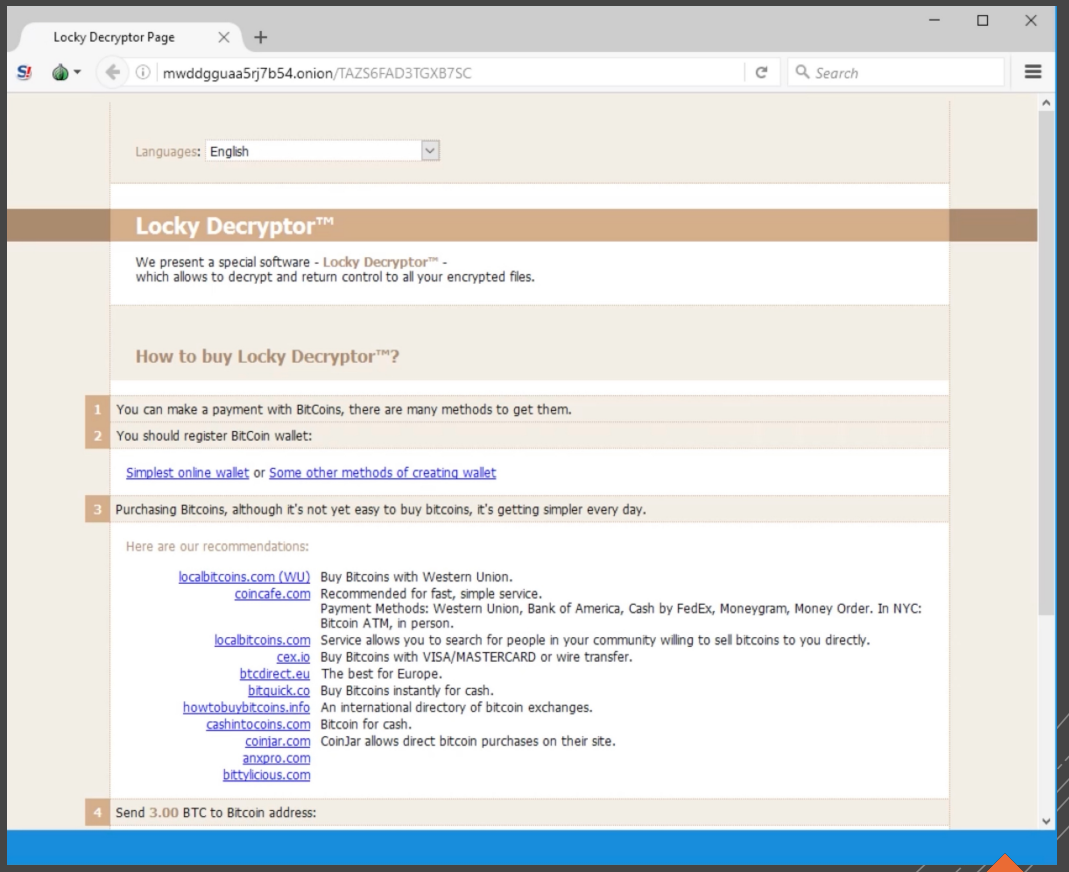


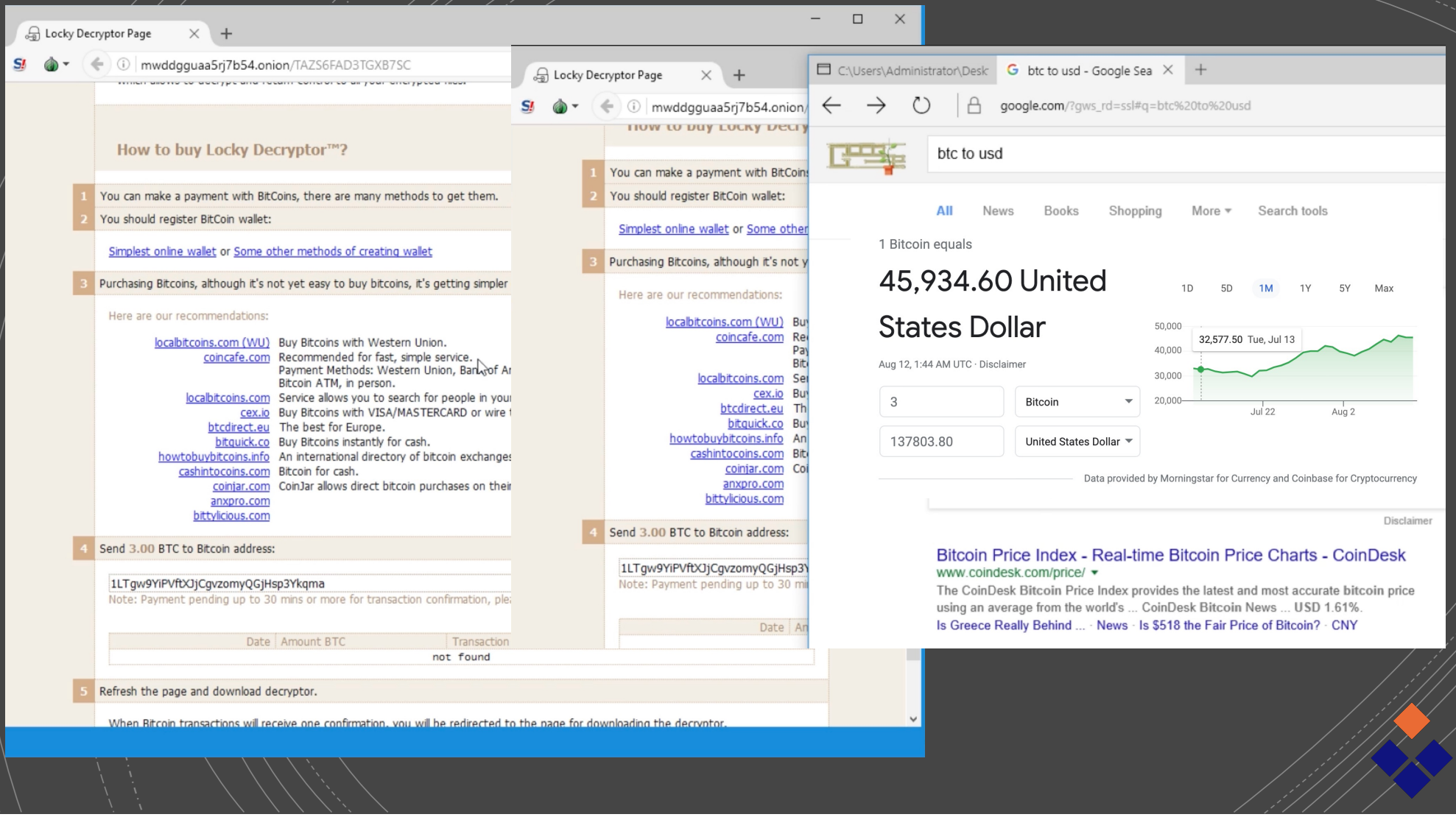

Documents
File
Home
Share
View
This PC
Documents
Search Documents
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows (C:)
Name
Custom Office Templates
Outlook Files
unpaid_contact
dank_meme.jpg
IDG_Example.pst
IMPORTANT_FILE.docx
IMPORTANT_PRESENTATION.pptx
unpaid_contact.zip
WE_HAVE_NO_MONEY.xlsx
-snk-465225987.js
Open File - Security Warning
Do you want to open this file?
Name: C:\Users\Administrator\Documents\-snk-465225987.js
Publisher: Unknown Publisher
Type: JavaScript File
From: C:\Users\Administrator\Documents\-snk-465225987.js
Open
Cancel
Always ask before opening this file
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?


-INSTRUCTION.bmp - Photos
View all photos
==+=+=_~~=-==
!!! IMPORTANT INFORMATION !!!!
All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: mwddgguaa5rj7b54.onion/TAZS6FAD3TGXB7SC
4. Follow the instructions on the site.
!!! Your personal identification ID: TAZS6FAD3TGXB7SC !!!
__*=$~.*=-*-_+*.+
|~__=*
|=_+__+=.+
~|=*+_~-+-


Drive Tools
Removable Disk (E:)
File
Home
Share
View
Manage
This PC
Removable Disk (E:)
Search Removable Disk (E:)
Documents
Pictures
Music
Videos
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows (C:)
Removable Disk
Network
Name
Date modified
Type
Size
_0-INSTRUCTION.html
11/30/2016 3:41 PM
HTML File
9 KB
TAZS6FAD-3TGX-B7SC-3FB0-CC442EB2EAF6.zzzzz
11/30/2016 3:41 PM
ZZZZZ File
16 KB
TAZS6FAD-3TGX-B7SC-4574-D7EB9C8AE2E6.zzzzz
11/30/2016 3:41 PM
ZZZZZ File
32 KB
TAZS6FAD-3TGX-B7SC-9642-661CED6E99A6.zzzzz
11/30/2016 3:41 PM
ZZZZZ File
73 KB
TAZS6FAD-3TGX-B7SC-B237-B6C221A2ACA1.zzzzz
11/30/2016 3:41 PM
ZZZZZ File
42 KB
TAZS6FAD-3TGX-B7SC-EA79-A502F7286D9C.zzzzz
11/30/2016 3:41 PM
ZZZZZ File
20,354 KB


Connecting...
Search or enter address
Search
HTTPS Everywhere is now active. You can toggle it on a site-by-site basis by clicking the icon in the address bar.
FAQ...
Tor Browser 6.0.7
A Network of People Protecting People
Tor is at the heart of Internet freedom
Donate Now! »
Welcome to Tor Browser
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Search securely with Disconnect.me.
What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.
You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
Run a Tor Relay Node »


Locky Decryptor Page
mwddgguaa5rj7b54.onion/TAZS6FAD3TGXB7SC
Search
Languages: English
Locky Decryptor™
We present a special software - Locky Decryptor™ -
which allows to decrypt and return control to all your encrypted files.
How to buy Locky Decryptor™?
1 You can make a payment with BitCoins, there are many methods to get them.
2 You should register BitCoin wallet:
Simplest online wallet or Some other methods of creating wallet
3 Purchasing Bitcoins, although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:
localbitcoins.com (WU) Buy Bitcoins with Western Union.
coincafe.com Recommended for fast, simple service.
Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, in person.
localbitcoins.com Service allows you to search for people in your community willing to sell bitcoins to you directly.
cex.io Buy Bitcoins with VISA/MASTERCARD or wire transfer.
btcdirect.eu The best for Europe.
bitquick.co Buy Bitcoins instantly for cash.
howtobuybitcoins.info An international directory of bitcoin exchanges.
cashintocoins.com Bitcoin for cash.
coinjar.com CoinJar allows direct bitcoin purchases on their site.
anxpro.com
bittylicious.com
4 Send 3.00 BTC to Bitcoin address:


Locky Decryptor Page
mwddgguaa5rj7b54.onion/TAZS6FAD3TGXB7SC
How to buy Locky Decryptor™?
1 You can make a payment with BitCoins, there are many methods to get them.
2 You should register BitCoin wallet:
Simplest online wallet or Some other methods of creating wallet
3 Purchasing Bitcoins, although it's not yet easy to buy bitcoins, it's getting simpler
Here are our recommendations:
localbitcoins.com (WU) Buy Bitcoins with Western Union.
coincafe.com Recommended for fast, simple service.
Payment Methods: Western Union, Bank of A
Bitcoin ATM, in person.
localbitcoins.com Service allows you to search for people in you
cex.io Buy Bitcoins with VISA/MASTERCARD or wire
btcdirect.eu The best for Europe.
bitquick.co Buy Bitcoins instantly for cash.
howtobuybitcoins.info An international directory of bitcoin exchange
cashintocoins.com Bitcoin for cash.
coinjar.com CoinJar allows direct bitcoin purchases on thei
anxpro.com
bittylicious.com
4 Send 3.00 BTC to Bitcoin address:
1LTgw9YiPVftXJjCgvzomyQGjHsp3Ykqma
Note: Payment pending up to 30 mins or more for transaction confirmation, ple
Date Amount BTC Transaction
not found
5 Refresh the page and download decryptor.
When Bitcoin transactions will receive one confirmation, you will be redirected to the page for downloading the decryptor.
Locky Decryptor Page
mwddgguaa5rj7b54.onion/
1 You can make a payment with BitCoin
2 You should register BitCoin wallet:
Simplest online wallet or Some other
3 Purchasing Bitcoins, although it's not y
Here are our recommendations:
localbitcoins.com (WU)
coincafe.com
localbitcoins.com
cex.io
btcdirect.eu
bitquick.co
howtobuybitcoins.info
cashintocoins.com
coinjar.com
anxpro.com
bittylicious.com
4 Send 3.00 BTC to Bitcoin address:
1LTgw9YiPVftXJjCgvzomyQGjHsp3Y
Note: Payment pending up to 30 mi
Date
C:\Users\Administrator\Desk
btc to usd - Google Sea
google.com/?gws_rd=ssl#q=btc%20to%20usd
btc to usd
All News Books Shopping More Search tools
1 Bitcoin equals
45,934.60 United States Dollar
Aug 12, 1:44 AM UTC · Disclaimer
3
Bitcoin
137803.80
United States Dollar
1D 5D 1M 1Y 5Y Max
50,000
40,000
30,000
20,000
32,577.50 Tue, Jul 13
Jul 22
Aug 2
Data provided by Morningstar for Currency and Coinbase for Cryptocurrency
Disclaimer
Bitcoin Price Index - Real-time Bitcoin Price Charts - CoinDesk
www.coindesk.com/price/
The CoinDesk Bitcoin Price Index provides the latest and most accurate bitcoin price using an average from the world's ... CoinDesk Bitcoin News ... USD 1.61%.
Is Greece Really Behind ... · News · Is $518 the Fair Price of Bitcoin? · CNY

Now What?

- A hacker has stolen your data and is holding it for ransom, will you pay?
- How will you respond to customers if their information is stolen?
- How will you operate without access to your entire network? Paper and pencil?

Pay or Don't Pay?

- 45% of all companies hit by ransomware pay the demanded amount. (Source: Imperva)
- The bad news is that 17.5% of all infected companies paid the ransom, yet still lost their data.
- Good news is 44.4% didn't pay the ransom, but still managed to recover their data. (Source: Agari)
- Even for companies who do pay the ransom there are still significant impacts. For many companies, the actual ransom payment isn't even the most expensive part of the attack. Companies have to restore backups, rebuild systems, work with forensic investigators to ensure that the hackers are truly locked out and, in many cases, implement stronger cybersecurity controls to prevent future attacks.

Why Your Business?

1. Lack of Cybersecurity Systems
2. Untrained Employees
3. Unsecured Accounts
4. Insufficient Upkeep
5. Lack of an Action Plan

Costs

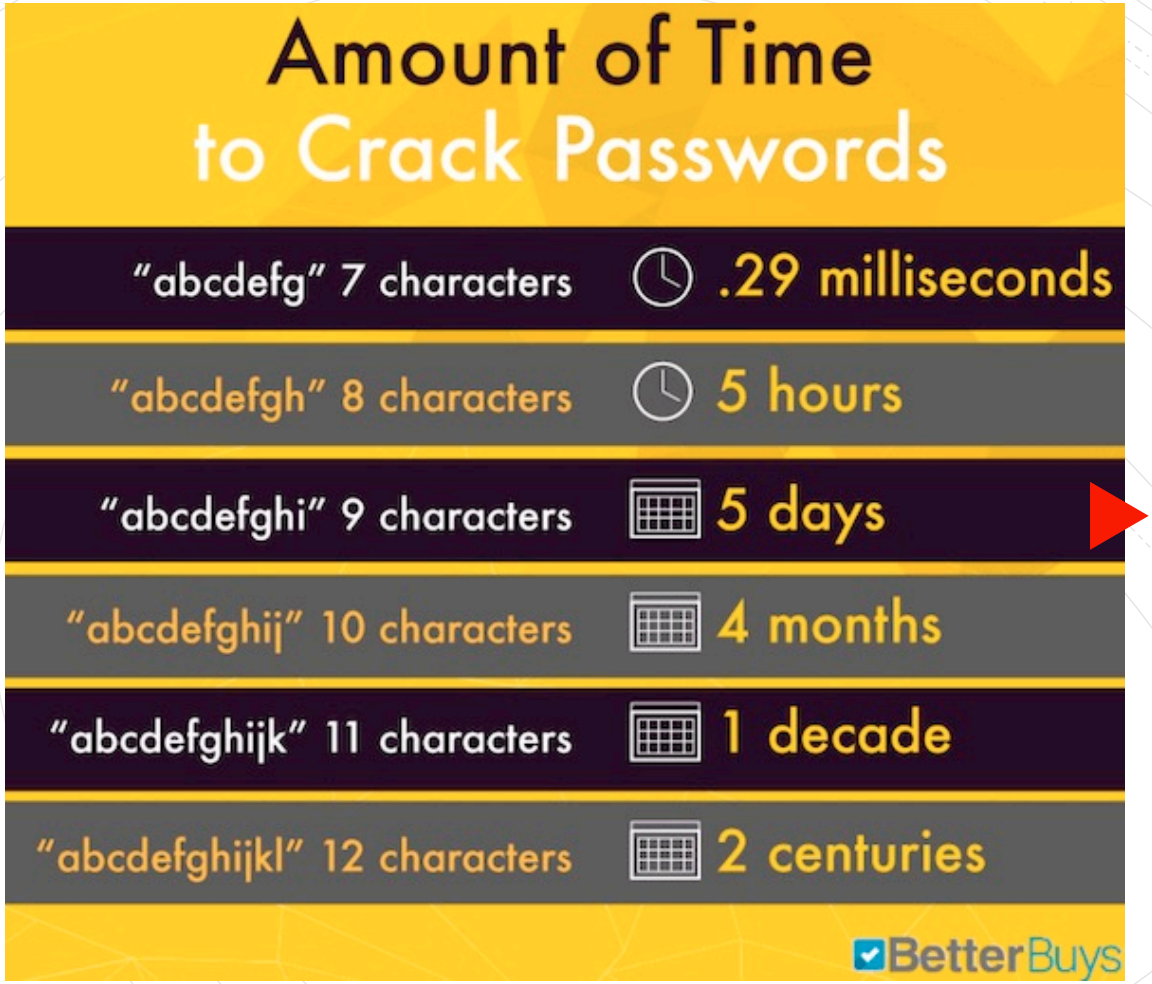
- 1. Forensic Audit
  In most cases, firms will need to conduct a forensic audit to determine how they were infiltrated. Audits can cost anywhere from $10k to over $100k, depending on the size of the business.
- Fines
  In many cases where customer data is leaked, the businesses can be fined tens of thousands of dollars for the breach.
- Ransom
  And then there are the potential costs of a cybercriminal asking for a hefty ransom in exchange for your leaked files.
- Recovery
  Possibly new computers, new software, training. 20 days – 6 months to be fully operational again.

Phishing

- **Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment.** They may:
  - say they've noticed some suspicious activity or log-in attempts
  - claim there's a problem with your account or your payment information
  - say you must confirm some personal information
  - include a fake invoice
  - want you to click on a link to make a payment
  - say you're eligible to register for a government refund
  - offer a coupon for free stuff

Do Today

- Require long varied passwords for all systems
- Enable two-factor authentication for any sensitive accounts
- Limit employees' access to sensitive data



People are the weakest link. Make sure to use uppercase, lowercase, numbers, special characters. Reset company passwords monthly. Multi-factor identification.

Do Tomorrow

There is Hope.

According to an East Coast Ski Area IT professional who wishes to remain anonymous, they recommend every ski area should be doing the following:

- Appoint an Executive level point person to lead your cybersecurity initiative.
- Have a current cyber action plan that starts with a current assessment of your systems to look for security holes and gauge your PCI (Payment card industry) compliance.
- Consider cyber insurance (if you can get it). There are pros and cons to cyber insurance, but it is recommended if done right. Tyson from Gregory & Appel.
- Invest in user training and spoofing services. Training employees needs to be an ongoing focus. 1Risk offers good material and services.
- Lastly, hire security professionals either in house or 3rd party but dedicate the resources for 24x7x365 monitoring and software tools.

Resources

- Internet Crime Complain Center
- https://www.ic3.gov/
- https://www.fbi.gov/scams-and-safety
- https://www.consumer.ftc.gov/features/feature-0038-onguardonline
- https://www.fbi.gov/news/stories/ic3-logs-6-million-complaints-051721
- https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa
- https://go.cyberready.com
- https://www.verizon.com/business/products/security/cyber-risk-mana gement/cyber-risk-monitoring/security-assessment-tool/security-assessment-signup/

Questions?

nxtconcepts

FOR A COPY VISIT NXTCONCEPTS.COM

https://nxtconcepts.com/ideas/seminars

MARKETING, WEB, DESIGN, INTERACTIVE, MEDIA