

You've Been Hacked!



You are at a bigger risk than you think



Cleatus Davis
Owner



Perception Versus Reality


- We perceive our networks are configured correctly.
- We believe we are secure.
 - We have anti-virus, so we are protected
- **We are wrong**

**79% of businesses were
hacked in 2016!**

Research by the CyberEdge Group



Most internet users can
correctly answer questions
< 50% of the time on a
knowledge quiz about
cybersecurity issues and
concepts. – *Pew Research Center*



60% of attacks target small businesses

Sources: Ponemon; Symantec; Nat'l Small Bus. Assoc.



55% of businesses <\$10M
report 1 or more breaches

- > 50% compromised more than once

Sources: Ponemon; Symantec; Nat'l Small Bus. Assoc.



- Cost of avg. attack on Small Business:
 - \$8,699 in 2013
 - \$20,752 in 2014

Sources: Ponemon; Symantec; Nat'l Small Bus. Assoc.



33% of firms required 3+ days
to recover from attack

Sources: Ponemon; Symantec; Nat'l Small Bus. Assoc.



The moment you log on to the internet, your computer starts its game of Russian roulette.

The personal data you store on your hard drive is a magnet for hackers and cybercriminals, and they will stop at nothing to break into your system.

Sources: Fox News, Kim Komando





The bad guys bet on you being unprepared and confused.



Research shows that most businesses “do not possess adequate time, nor resources to actively tackle the issues of information security.”

source: “Managed Information Security in Small and Medium Sized Enterprise: A Holistic Approach” –Tawileh, Hilton, McIntosh



Hackers are not mischievous teenagers anymore.



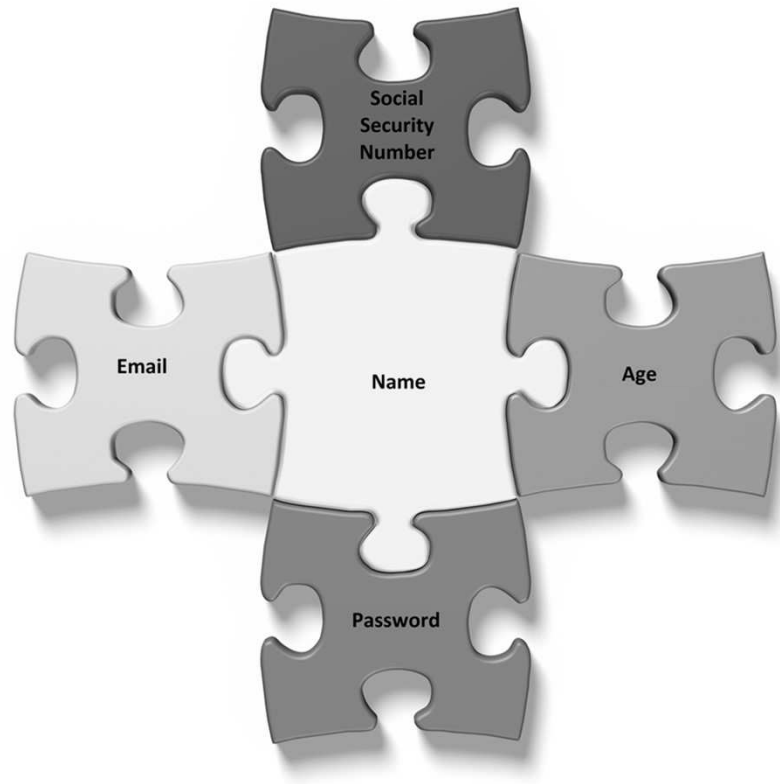
Viruses, Phishing, Ransomware & Identity Theft are about Money



Today's threats are about gathering information and gaining access.

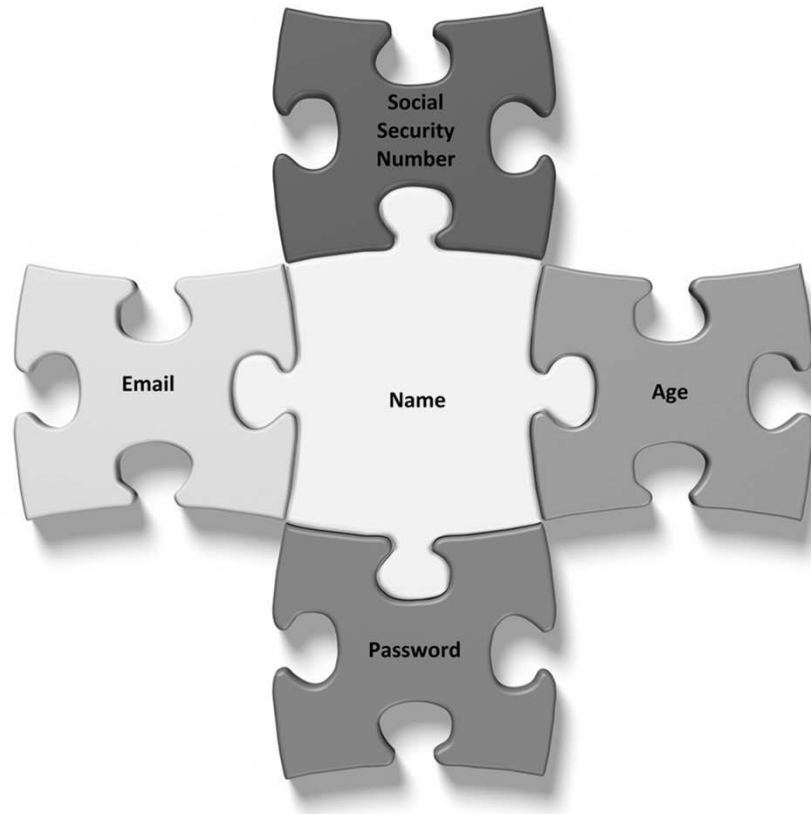


Identity Theft is Like a Puzzle



The more pieces of information that a criminal can gather about you, the easier it is to steal or manipulate your identity.

Identity Theft is Like a Puzzle



You must protect

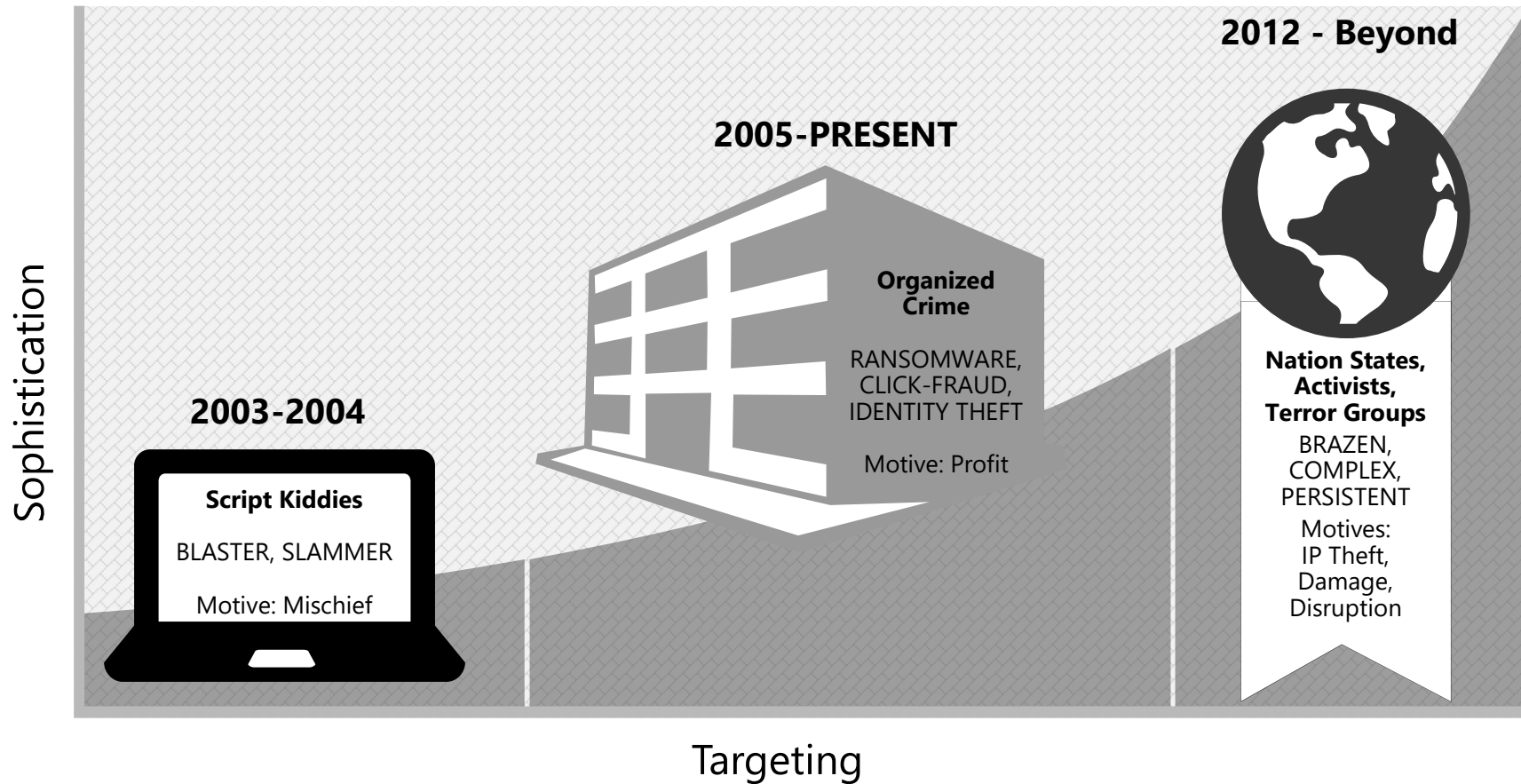
- Your personal information
- Your business information
- Personal Information entrusted to you by others

More Types of Threats

More Complex Threats

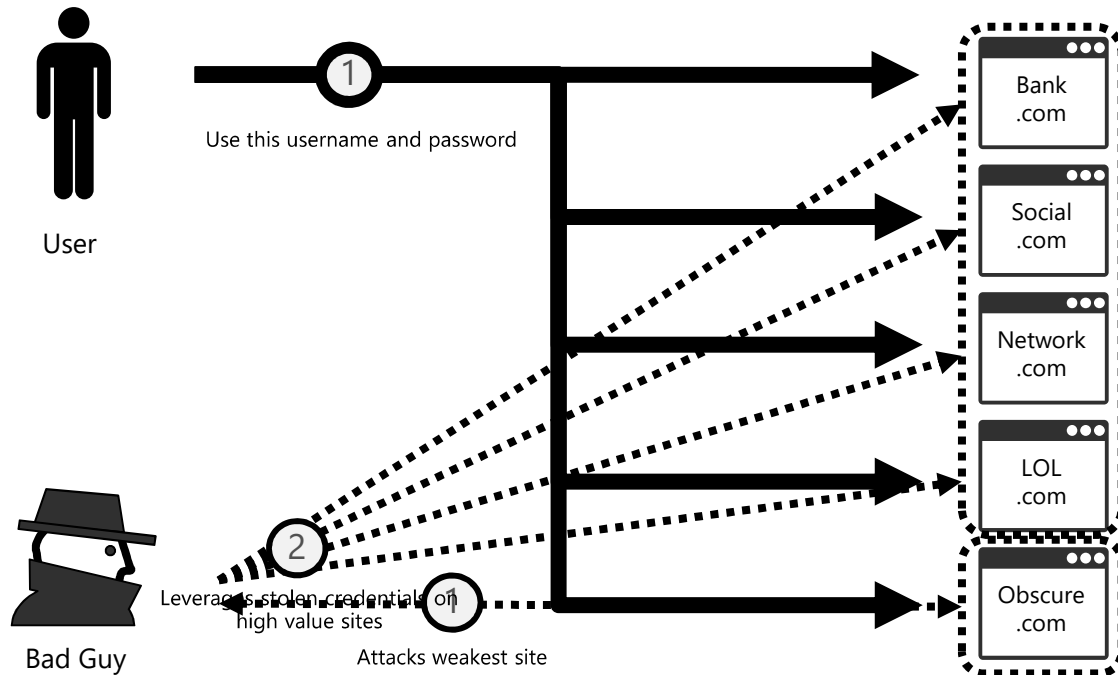


THE EVOLUTION OF ATTACKS

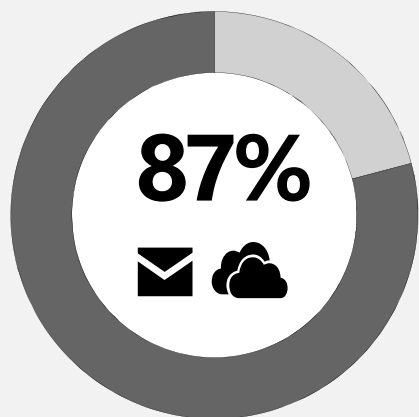


Internet username and password

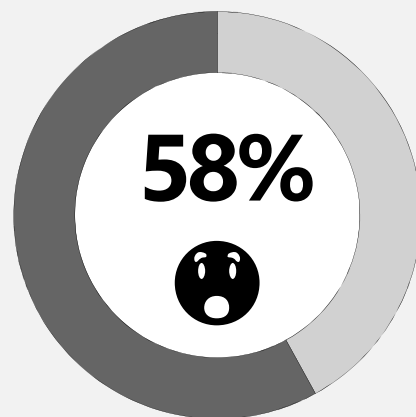
THE USER & SITES WE USE ARE A WEAK LINK



Data Leakage



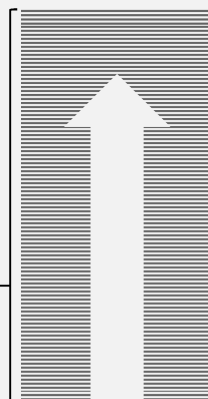
...of senior managers admit to **regularly** uploading work files to a personal email or cloud account¹



Have accidentally sent sensitive information to the **wrong person**¹

\$240

PER
RECORD



Average per record **cost of a data breach** across all industries²

¹Stroz Friedberg, "On The Pulse: Information Security In American Business," 2013

²HIPPA Secure Now, "A look at the cost of healthcare data breaches," Art Gross, March 30, 2012

Information protection needs

DEVICE PROTECTION

Protect system and data when device is lost or stolen

DATA SEPARATION

Containment
BYOD separation

LEAK PROTECTION

Prevent unauthorized apps from accessing data

SHARING PROTECTION

Protect data when shared with others, or shared outside of organizational devices and control

How Do We Stay Safe?

- Prevention
- Process



Prevention

- Use the Right Technology
- Have & Follow Processes
- Train Your Users



Right Technology


The type of threats have changed.
Just having a basic anti-virus program isn't enough.



Right Technology

**The type of threats have changed
Just having a basic anti-virus program
isn't enough**

You need:

- Full Featured Business Class Router to protect your network
 - Full Featured Business Class Anti-Virus/Anti-Malware
 - Business Class email with spam protection
 - Follow standard security recommendations
 - Use vulnerability scanning to find holes in your computers and network
- 

Right Technology

- Full Featured Business Class Router to protect your network
 - The modem router combination device from you internet provider does not really protect your network.
- What you need
 - Advanced firewall
 - Intrusion Detection
 - Real time traffic scanning
 - Web access filtering
 - File download scanning and filtering



Right Technology

- Full Featured Business Class Anti-Virus/Anti-Malware
 - No Freebie software
 - Best protection (Bitdefender, Kaspersky, Norton)
 - More than basic Anti-Virus
 - Must update automatically and frequently (multiple times per day)
 - Should be password protected

Right Technology

- Business Class email with spam protection
 - Don't use free email account from your internet service provider
 - Generally not secure
 - Ad supported (major source of malware and viruses)
 - Does not look professional
 - If your email ends with yahoo.com, sbcglobal.net, att.net, gmail.com, cox.net, cableone.net, etc.....It is not a business quality account.
 - Need Spam Filtering
 - Recommend Email Archiving

Free Email accounts are not secure!

- **You are not the customer.** The Email Provider makes money from advertisers and data miners who use your information to make more money off of you.
- **Advertisements** in free email are a common source of viruses, malware and scams. This means that by just checking your email you are increasing your chances of getting a virus or being a victim of a scam.
- **Spam filtering** on free accounts is very limited or is not available. This means that you get a lot of junk mail. Often this junk mail contains viruses, it can also be a source of scams and attempts to gain access to your information by phishing.
- **Hacked** - Many of these free email providers have been hacked, sometimes repeatedly.

Business Quality Email

- **You are the customer.** The Email Provider makes money from you and gets paid to deliver a quality product.
- **No Advertisements** - Business email accounts do not have advertisements on your email account.
- **Spam filtering** – Removes the junk mail. Optionally, can also scan and remove viruses, phishing scams and bad links.
- **Archiving** – keeps a backup copy of every email for compliance, public records requests and prevents deletion of emails by accident or mischief.



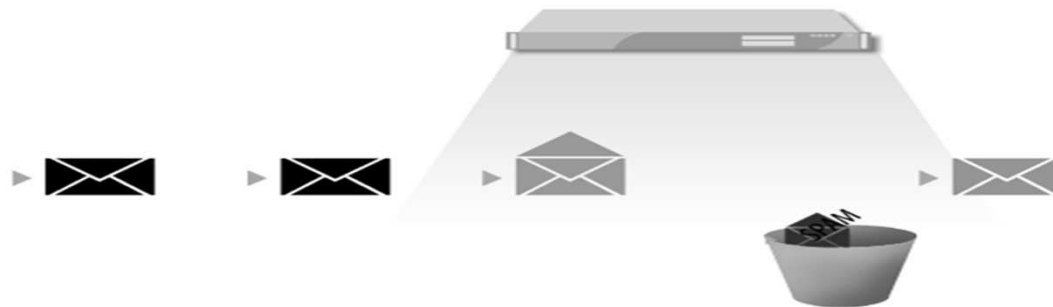
A black and white photograph of a person wearing a black balaclava, with only their eyes visible through the eye holes. They are holding a flashlight, which is turned on, casting a bright beam of light. The background is dark and indistinct.

Email threats:
Spam
Malware
Phishing
Confidential leaks
Compliance


Email Security

Protecting business communications

- Scan inbound and outbound email and identify
 - bad mail (Spam, Viruses, Phishing, etc...)
 - mail containing confidential information (document leakage)
- Apply business rules to block, quarantine or encrypt
- Automatic Archival of all email for compliance



Right Technology

- Follow Proper Security Standards
 - All computers should use a proper password
 - Users operate under a “limited” account instead of “administrator” account.
 - Routinely clean your computer and remove any unnecessary programs
 - Keep updates current for Windows, programs and security
 - Do not install any software unless you are 100% sure you need it
 - If you have wifi at your office make sure it has security enabled and only office staff with a need to use it are connected.
 - Do not use public wifi when traveling
- 

Be Prepared


- Have a good Backup & Recovery process



Perception Versus Reality

- We perceive our networks are configured correctly.
- We believe we are secure.
 - We have anti-virus, so we are protected
- **We are often wrong**

Vulnerability Scanning


- Checks for issues that might otherwise go unnoticed
 - Checks for unsecured sensitive data
 - Date of Birth
 - Social Security Number
 - Credit Cards
 - Checks for unsecured ports
 - Checks for changes in security
- 

Process

- Procedures
- Policy
- Train Your Users



Procedures

- Users don't install new programs and/or updates.
 - File sharing is limited to a single shared folder on 1 computer and does not use the built in "Everyone" group.
 - Local documents are stored in the user's My Documents folder.
 - All shared documents are located on a shared drive with appropriate permissions for viewing and changing based on User.
 - Do not use USB sticks for sharing files.
 - Don't install any software unless you are 100% sure you need it.
 - Don't let other people use your computer.
 - Don't open suspicious emails.
 - Don't share your private information.
- 

Policy

- You need Technology/Computer Use Policies
 - Your computers are tools, not toys
 - Spell out what is proper and improper use of Housing Authority Computers
 - Spell out proper and improper use of the Housing Authority Network
 - Password Policy
 - Disaster Recovery Plan
 - Enforce your policy


Train Your Users Frequently

- Users need to know your policy
- Be aware of new threats
- Make sure everyone knows what to do if something bad happens

Be Suspicious



Summary

- Anti-virus & backup are a good start, but there is much more to do if you want to be secure
 - Do not use free email accounts
 - Use business class technology tools, not consumer or home versions
 - Treat your technology like tools, not toys
 - Create policies and procedures about security and train your users.
- 

Let Us Help You!



UltimateITGuys.com
