Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat
In New York, data breaches shot up 60% last year

On Tuesday, the office of New York State Attorney General Eric T. Schneiderman released a summary of the year 2016 in data breaches. Collecting any breach that affected New York state residents, the Attorney General’s office saw those numbers swell by 60 percent overall last year. While hacking accounted for more than 40 percent of the 1,282 total incidents reported, employee negligence, including inadvertent exposure and device loss, was close behind at 37 percent.

"In 2016, New Yorkers were the victims of one of the highest data exposure rates in our state’s history," Attorney General Schneiderman said in a statement on the report. “The total annual number of reported security breaches increased by 60% and the number of exposed personal records tripled... It’s on all of us to guard against those who try to use our personal information for harm — as these breaches too often jeopardize the financial health of New Yorkers and cost the public and private sectors billions of dollars.”

Awareness

- A lack of security appreciation contributes directly to poor security awareness, most notably at the personnel level.
  - This is one of the leading contributors to the human error factor with most security breaches.
  - Security needs to be everyone’s business.
  - Corporations and government agencies are directly responsible for protecting personal information entrusted to them by their consumers, so measures must be taken to increase awareness in the everyday IT environment.
  - The most critical step to changing user behavior is to build a secure-minded culture from the ground up.
  - To create this culture, all employees need to be educated and tested on security threats and how their day-to-day computer use behavior can affect their organization’s security posture.

CIO Magazine
Social Engineering

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim.

THERE IS NO PATCH FOR HUMAN GULLIBILITY

- Lose something
- Gain something
- Fear/greed
- “Principles of Influence”
  Influence: The Psychology of Persuasion
- email
- telephone
- in person
- Trojan horse/Watering holes
- Thieves pose as You
- Spouse
- Bill collector
- Bank
- Utility
- Merchant / Organization
- Fellow employee
- Government agency
- Landlord

Strip-search hoax plagues fast-food outlets

Caller poses as police, falsely warns managers of thief on premises

By Mitch Stacy, Associated Press | April 10, 2004

The caller to the Phoenix-area Taco Bell said he was a police officer and informed the manager there was a thief on the premises. Someone’s pocketbook was missing, the caller said, ordering that a female customer be detained and strip-searched in a back office.

But there was no theft. Investigators believe the caller was an impersonator, possibly from north Florida, who has pulled the same stunt dozens of times nationwide since 1999 with alarming success.

The caller, who sometimes poses as a company official, has persuaded managers at restaurants and other stores to detain and search employees for drugs or money. Targets have included Taco Bell, McDonald’s, Wendy’s, Burger King, Ruby Tuesday, Applebee’s, Perkins, and others.
People Are Still Dumb Enough to Pick Up Abandoned USBs and Plug Them In

Stuxnet delivered to Iranian nuclear plant on thumb drive

Citing U.S. intelligence sources, ISSSource says an infected memory stick was used to hit the facility with the worm that severely damaged Iran's nuclear program.

An Iranian double agent working for Israel used a standard thumb drive carrying a deadly payload to infect Iran's Natanz nuclear facility with the highly destructive Stuxnet computer worm, according to a story by ISSSource.
Scour all of the social networking sites for employees of target company like LinkedIn, Twitter, and Facebook.com

Find numerous people who openly discussed what they did for a living

Create a Facebook group site identified as “Employees of” the company.

Using a fictitious identity proceed to “friend,” or invite, employees to our “company” Facebook site. Membership grows exponentially each day.

By creating a group, you access to employees profiles. The “group” is a place where those who you know, like and trust are your “Friends” and in this case fellow employees who you have no reason to distrust.

Chose to use the identity of one of our Facebook-friended employees to gain access to the building.

Relative to as companies size you may be able to recreate the identity of an employee that’s not known to the branch office to breach. But the name needs to be in the system.

With a little creativity, a fake business card and enough information gleaned off of Facebook, you’re in.
FBI warns of dramatic increase in business e-mail scams

FBI Phoenix
April 04, 2016

FBI officials are warning potential victims of a dramatic rise in the business e-mail compromise scam or “B.E.C.,” a scheme that targets businesses and has resulted in massive financial losses in Phoenix and other cities.

The schemers go to great lengths to spoof company e-mail or use social engineering to assume the identity of the CEO, a company attorney, or trusted vendor. They research employees who manage money and use language specific to the company they are targeting, then they request a wire fraud transfer using dollar amounts that lend legitimacy.

There are various versions of the scams. Victims range from large corporations to tech companies to small businesses to non-profit organizations. Many times, the fraud targets businesses that work with foreign suppliers or regularly perform wire transfer payments.

- Law enforcement globally has received complaints from victims in every U.S. state and in at least 79 countries.
- From October 2013 through February 2016, law enforcement received reports from 17,642 victims.
- This amounted to more than $2.3 billion in losses.

Barbie-brained Mattel exec phell for phishing, sent $3m to China

Hackers scoped internal structures to figure out who had authority to send funds

6 Apr 2016 at 06:58, Darren Pauli

Toy maker Mattel has recovered some US$3 million it shipped off to Chinese hackers who sent a well-crafted phishing email to a finance executive.
Cybercriminals sneak in to realty deals and sneak out with $100,000 or more

Watch Out, Your Closing Funds May Be Heading to a Cybercriminal

While no one knows the exact number of victims or extent of the problem, the National Association of Realtors® in Chicago told the Post that this scam has hit “hundreds, if not thousands,” of home closings. It’s become serious enough, in fact, that on March 18, the Federal Trade Commission issued a warning to home buyers. As for what’s fueling this trend, some experts we spoke to point to the relatively lax security in the world of real estate compared with other financial industries.

“It was just a matter of time until scammers recognized the opportunity to target real estate agents and their clients,” says Robert Siciliano, CEO of IDTheftSecurity.com. “Currently, most industries that have experienced large data breaches have put systems in place and have become hardened. That means the real estate industry and others become the path of least resistance. Unlike the entire financial industry who have encrypted communications, the real estate industry is a hodgepodge of free email accounts and unprotected communications.”

Scammers phish for mortgage closing costs

March 18, 2016
by Colleen Tressler
Consumer Education Specialist, FTC

Buying a home is exciting. You saved for the down payment, scheduled the move, and are dreaming of planting new roots. Closing is right around the corner... unless a scammer gets your settlement fees first.

The Federal Trade Commission and the National Association of Realtors® are warning home buyers about an email and money wiring scam. Hackers have been breaking into some consumers’ and real estate professionals’ email accounts to get information about upcoming real estate transactions. After figuring out the closing dates, the hacker sends an email to the buyer, posing as the real estate professional or title company. The bogus email says there has been a last minute change to the wiring instructions, and tells the buyer to wire closing costs to a different account. But it’s the scammer’s account. If the buyer takes the bait, their bank account could be cleared out in a matter of minutes. Often, that’s money the buyer will never see again.
**Definition:** Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

**Data Breaches**

- Irresponsible/malicious insiders
- 3rd party fault
- Laptop theft
- Physical security vulnerabilities
- Loss
- Hacking: 21st century burglary
Russian Hackers Have 270 Million Email Logins, Including Gmail and Yahoo Accounts

Cluster of “megabreaches” compromises a whopping 642 million passwords

MySpace, Tumblr, and Fling are the latest services to join discredited LinkedIn.
Dictionary attacks: These rely on software that automatically plugs common words into password fields. Password cracking becomes almost effortless with a tool like John the Ripper or similar programs.

Cracking security questions: When you click the "forgot password" link within a webmail service or other site, you’re asked to answer a question or series of questions. The answers can often be found on your social media profile. This is how Sarah Palin’s Yahoo account was hacked.

Simple passwords: When 32 million passwords were exposed in a breach last year, almost 1% of victims were using "123456." The next most popular password was "12345." Other common choices are "111111," "1234567," "12345678," "123456789," "princess," "qwerty," and "abc123." Many people use first names as passwords, usually the names of spouses, kids, other relatives, or pets, all of which can be deduced with a little research.

Reuse of passwords across multiple sites: Reusing passwords for email, banking, and social media accounts can lead to identity theft. Two recent breaches revealed a password reuse rate of 33% among victims.

Social engineering: Social engineering is an elaborate type of lying. An alternative to traditional hacking, it is the act of manipulating others into performing certain actions or divulging confidential information.

There are a number of ways to create more secure passwords. One option is to create passwords based on a formula, using a familiar name or word, plus a familiar number, plus the first four words of the website where that password will be used. Mix in a combination of upper and lowercase letters, and you have a secure password. Using this formula, your Bank of America password could be “Dog?Bank;” for example. (Add one capital letter and an asterisk to your password, and it can add a couple of centuries to the time it would take for a password cracking program to come up with it.)
Hacking for Money

- Social engineering
- Phishing
- Weak credentials
- Insecure passwords
- NO PASSWORDS

La Bellissima Mafiosa
Hi Rob,
I'm not sure if you saw what had happened on my FB Page last night, but someone stole my cell phone while I was at a concert, and posted all of my naked pictures off of my phone and posted them to my wall. They were up there for hours. 😞
Is there anyway you could help me find out who it was?
50-75 YEAR OLDS!

Flawed System

SSN + Credit + Fake ID
Legal Forms of ID Circulating

- 49 versions of Social Security card
- 14,000 types of birth certificates
- 200 plus forms of driver’s licenses
- 14 states no photo
- Signature?

What is a signature?
1. Print Out This Document
2. Fill Out The Information
3. Choose an ID Package
4. Make sure you sign the disclaimer and sign in the box
5. Give picture with a head shot of about 1” x 1”, passport photo work best
6. Send the completed information, your payment, and a check or money order made payable to ‘Cash’ to the address at the bottom. All prices are in US Dollars.

### Novelty ID Info:

<table>
<thead>
<tr>
<th>Last Name</th>
<th>First Name</th>
<th>Middle Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date Of Birth</td>
<td>Height</td>
<td>Weight</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sign your name within the box below

---

**Disclaimer**

- ID Theft Security is not responsible for any misuse of the novelty IDs. It is the responsibility of the user to use the novelty IDs for legal and ethical purposes only. The use of novelty IDs for illegal or unethical purposes may result in legal consequences.
- ID Theft Security is not responsible for any consequences resulting from the use of novelty IDs. The user is solely responsible for the consequences of their actions.
- ID Theft Security reserves the right to refuse service to anyone at any time for any reason.

---

**Shipping Options**

<table>
<thead>
<tr>
<th>Option (Name Circle One)</th>
<th>Charge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard - Free</td>
<td></td>
</tr>
<tr>
<td>Rush - $30</td>
<td></td>
</tr>
</tbody>
</table>

Send To: Affelte De Qualité, Fuerstenstrasse 103, 80799 Munich Germany

---

**Pricing:**

- Novelty ID - $250
- Novelty ID - $275
- Novelty ID - $300
- Novelty ID - $325
- Novelty ID - $350
- Novelty ID - $375
- Novelty ID - $400
- Novelty ID - $425
- Novelty ID - $450
- Novelty ID - $475
- Novelty ID - $500
- Novelty ID - $550
- Novelty ID - $600
Identity Theft Types

- **New Account Fraud**
  Using another’s personal identifying information (SSN) to obtain products and services using that person’s good credit standing

- **Account Takeover Fraud**
  Using another person’s account numbers such as a credit card number to obtain products and services using that person’s existing accounts or extracting funds from a person’s bank account.

- **Tax Identity Theft**
  Tax-related scams have increased by over 700% since 2008. Two million fraudulent tax returns were filed in 2011 alone, at a cost of two billion dollars.

- **Child Identity Theft**
  Studies show child identity theft is affecting over 500,000 kids every year.

---

Identity Theft Types

- **Medical Identity Theft**
  The deadliest form of identity theft. 1.5 Million victims every year. The motivation of the thief is medical procedures or any form of attention regarding healthcare

- **Criminal Identity Theft**
  Someone commits a crime and uses the assumed name another person. The thief in the act of the crime or upon arrest poses as the identity theft victim.

- **Business or commercial identity theft**
  Using a business’s name to obtain credit or even billing those businesses clients for products and services.

- **Identity Cloning**
  Encompasses all forms of identity theft. The thief is actually living and functioning as the victim on purpose
How a Thief Obtains the Parts

Mail

- Stealing incoming mail
- Stealing outgoing mail
- Incorrectly getting mail
- Changing mailing address

3/28/2017

How a Thief Obtains the Parts

Dumpster diving

- Going through your rubbish
- Someone-else’s rubbish

3/28/2017
How a Thief Obtains the Parts

Steal from your home - known - unknown
Steal a wallet or pocketbook
From Inside an organization

How a Thief Obtains the Parts
Covertly

From your license plate
Intercepting cordless or cellular transmissions
CID Spoof
Internet hacking
Phishing
Important Fraud Alert from Citibank
Citibank [citibank227@att.net]

Dear Citibank Account Holder,

On January 10th 2004 Citibank had to block some accounts in our system connected with money laundering, credit card fraud, terrorism and check fraud activity. The information in regards to those accounts has been passed to our correspondent banks, local, federal and international authorities.

Due to our extensive database operations some accounts may have been changed. We are asking our customers to check their checking and savings accounts if they are active or if their current balance is correct.

Citibank notifies all its customers in cases of high fraud or criminal activity and asks you to check your account’s balances. If you suspect or have found any fraud activity on your account please let us know by logging in at the link below.

Click Here To Login

Welcome to Citi.com - Microsoft Internet Explorer provided by Comcast
not an attachment; an embedded image that links out to a fake “sign in with Google” page
Spyware

- Scareware: Fake Anti-virus
- Ransomware: hold data for ransom
- Remote assistance scams
- Keyloggers: Spyware Software
- Keycatchers: Hardware

Spyware

The Gold Standard in Internet Monitoring and Surveillance Software
Spector Pro is the world's best selling software for monitoring and recording every detail of PC and Internet activity - in your home or in your office. Selected as the Editors' Choice by the experts at PC Magazine, Spector Pro contains seven integrated tools that record: chats, instant messages, emails sent and received, web sites visited, keystrokes typed, programs launched, peer to peer file searching and swapping - plus, Spector Pro provides the equivalent of a digital surveillance tape so that you can see the EXACT sequence of EVERYTHING your family members or employees are doing on the computer. All seven tools work together at the same time, secretly saving all the recordings in a hidden location only you know about.

Special Offer: $99.95
Regularly $149.95
KeyCatcher Mini 32K
32K KeyCatcher Keylogger
Shipped US Mail
Only $79
Click the Buy Now button below to order using PayPal

32K KeyCatcher Keylogger
Shipped Overnight
Only $104
Click the Buy Now button below to order using PayPal

A tiny device that records everything the person types.
No Software Needed
Cannot be detected by anti-spy softwares

Records up to 65,000 Keystrokes

If You Want Them Shipped to a Different Address please include Shipping Address in PayPal’s Notes
One year limited warranty
Return policy
Privacy Policy
ATM Skimming

Raw Data

http://www.youtube.com/watch?v=5zJRzSqad-A

Second Hand Devices

- Printers
- Craigslist
- 30 devices
- 30 mile radius of Boston
- Basic forensics
- Half provided data
Credit

- Check credit reports 3 times annually
- AnnualCreditReport.com
- Dispute inaccuracies
- Spouse/child credit report
- Credit monitoring
- Credit freeze
- Fraud alerts

Credit Freezes

- Locks credit
- Slows loan process
- State Security Freeze

https://www.experian.com/freeze/center.html
https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page
Credit Cards

- Check statements / refute unauthorized charges within 60 days
- Use credit cards instead of debit cards
- Pay attention to the expiration date of credit cards and look for arrival of new cards
- Sign all new cards immediately
- Destroy black carbon credit receipts
- Thin out your wallet

Shredding Data

- All throwaway documents - contract an authorized disposal company for secure disposal
- Ask all public and private entities about policies for disposal
- Opt out of and destroy pre-approved credit card offers
- Photocopy all documents in your wallet/purse
- Reconcile bills and statements diligently and timely
- Secure all receipts, legal documents and account numbers; tax docs, cancelled checks
- Unlist name and number from phonebook
- Eliminate paper statements
- Thoroughly erase data from discarded hard drives
  - www.killdisk.com or a sledge hammer
  - McAfee Shredder and Norton WipeInfo
Wireless Security

- Wi-fi is insecure
- 300-500 ft range
- Free wi-fi
- evil twins
- Secure Mobiles
- Virtual Private Network
- (VPN)
Anti-Virus

- Install virus protection and keep it automatically updated*
- Default configurations
- Beware of Scareware

Windows Update

Welcome
update your computer

Windows Update is looking for available updates...

Automatic Updates:
Turned OFF

Your computer is set to receive notifications when new updates are available.
Pick a time to install updates.

News

What to know before you install Windows XP Service Pack 2

Microsoft

2004 Microsoft Corporation. All rights reserved.
Be careful about which Web sites you visit. Sites devoted to illegal or questionable subjects, such as hacker sites, sites for downloading pirated music or software, and pornographic sites are most likely to contain malicious code.

Do not conduct financial transactions or send private information over the Web unless the site is secure (which is usually indicated by an HTTPS or a “lock” icon in the browser’s status bar).

Configure your browser’s security settings for safe browsing.

Configure your browser’s privacy settings to avoid unwanted cookies and pop-up ads.

Enable checking of digital signatures on drivers and other programs you download.

---

**Internet Browser**

- Background Checks: verify education, work experience, criminal histories.
- Dumb Terminals: PCs with no hard drives, email or printers. No cell phones, notebooks or pens.
- Automatic lockout: former employees are security risks
- Beef up access control
- Shred Shred Shred Shred Shred Shred
- Review policies for remote computing
- Shut down networks when not in use. 24/7 no good
The 5th media connecting television, radio, print and internet together. It has become the sole voice of the people and certain public facing businesses. Social Media is an essential tool for any businesses who wishes to develop or maintain a good relationship with the public.

Social Media is

Personally
• Fun/entertaining
• Maintain friends/contacts

Professionally
• Marketing/PR
• Network/Connect
• Customer service
• Publics ideas/suggestions
• Serious
Twitter hoax claiming that an explosion occurred at the White House injuring President Obama led to a 150-point drop, a $136 billion market value, in the Dow Jones industrial average.
Do: Beware of Dangers

- Cyberbullying
- Kidnappers
- Stalkers
- Thieves
- Terrorist
- Hackers/Phishers/Scammers
- Enemy organizations
- Pedophiles
- Sexting
- 750,000+ registered sex offenders
- 95,000 registered sex on MySpace
- [https://www.youtube.com/watch?v=6jMhMVEjEQg&feature=youtu.be](https://www.youtube.com/watch?v=6jMhMVEjEQg&feature=youtu.be)

27-Year-Old Spring Valley Man Facing Felony Charges After Allegedly Preying on 12-Year-Old

Spring Valley resident Scott Stilwell is facing two felony charges

By Samantha Tatro and Omari Fleming

---

**TRENDING STORIES**

1. **Video** Upcoming @ Nino W SoCal into 2016, Scripps

2. **Video** Wife Who Killed Husband Guilty of 2nd-Degree Murder

3. Weekend Events: Oct. 8-11

4. Former Beauty Queen Child Porn to Sheriff's Police

---

A 27-year-old Spring Valley man is under investigation for allegedly driving more than an hour away to prey on a 12-year-old girl, officials said.
MI6 chief blows his cover as wife's Facebook account reveals family holidays, showbiz friends and links to David Irving

By JASON LEWIS, MAIL ON SUNDAY SECURITY EDITOR
UPDATED: 13:14 EST, 5 July 2009

The new head of MI6 has been left exposed by a major personal security breach after his wife published intimate photographs and family details on the Facebook website.

Sir John Sawers is due to take over as chief of the Secret Intelligence Service in November, putting him in charge of all Britain’s spying operations abroad.

But his wife’s entries on the social networking site have exposed potentially compromising details about where they live and work, who their friends are and where they spend their holidays.

Amazingly, she had put virtually no privacy protection on her account, making it visible to any of the site’s 200million users who chose to be in the open-access ‘London’ network—regardless of where in the world they actually were.

There are fears that the hugely embarrassing blunder may have compromised the safety of Sir John’s family and friends.

How to Rob a bank using Social

Wait! What?!
12 Things NEVER do Online

1. Post illegal activities
2. Cyberbullying
3. Disrespecting anyone
4. Posting objectionable content
5. Posting private information
6. Posting location data
7. Lie/Cheat
8. Make threats
9. Post inappropriately
10. Post emotionally
11. Don’t copycat
12. Be so public

Don’t: Be Stupid

Physician terminated after Facebook comment
sues Spectrum

GRAND RAPIDS, MI – An emergency room doctor has sued Spectrum Health, saying her position was terminated and she was wrongfully accused of a HIPAA violation over a comment made on Facebook.

Dr. Catherine Ruetz, the former associate medical director of the emergency services, filed the suit Friday, March 14, in U.S. District Court against Spectrum Health hospitals and two executives – Kevin Spaine, president of the hospitals; and Jeanna Besche, vice-president.

The lawsuit involves a Facebook post made in August 2013.

Ruetz says she saw a picture Aug. 5, 2013, posted by an emergency department nurse that showed the backside of a woman. Believing she recognized the woman as someone she had seen in public and in the emergency department, Ruetz posted a comment on the photo: “OMG...is that TBT”

According to the lawsuit, the Facebook post and comments were investigated by Spectrum, and some employees were fired and some were not.

Ruetz said a nurse who posted “I like big butts and I cannot lie...” – an apparent nod to the popular 5’4” Min-A-Lot song – was only reprimanded, not fired.
Consequences

• 1 in 10 college admissions officers routinely check applicants’ social network pages
• 2 in every 5 applicants had information on social media sites that reflected poorly on them
• Get kicked off your sports team
• Miss a shot at going to your favorite college
• Get fired
• Get arrested
• Get cyber bullied
• Get stalked
• Get abducted
• Get assaulted
• Get killed
• Damaged reputation
• Get burglarized
• Identity theft
• One out of every five online divorce petitions filed involve FB