//CYBER.CRIME()

PHISHING.

Dylan Van Engelhoven

What is phishing?

(fish´ing) **(n.)** The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web-site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Types of phishing techniques.

- phishing-trying to acquire info such as usernames, passwords, etc. while pretending to be a trustworthy entity.
- spear phishing- attempts directed at a specific person or group. The attacker usually gathering info about the group/individual before beginning their attack.
- whaling- attacks directed specifically at high profile targets.

Whaling Example

Types Cont.

Some other types of phishing include

- clone phishing
- link manipulation
- filter evasion
- website forgery
- phone phishing
- tabnabbing
- evil twins

History of phishing.

- originated sometime around the year 1995
- 1996- the first time that the term phishing was used(on a Usenet newsgroup)
- 1997- AOL had hackers creating fake profiles and selling them to other hackers.
- 2001 - first known direct attempt on a payment system, E-gold.
- 2004 - recognized as a fully industrialized part of the economy of crime.

Phishing Hot Spots

1. US
2. Canada
3. Egypt
4. Germany
5. France
6. Romania
7. Netherlands
8. UK
9. Russia
10. Israel

Damaged caused by phishing.

- Leads to loss which ranges from the access of email to monetary loss.
- It also can give information such as: credit card numbers, social security numbers, and other information that one would not want others to have.
- In between may 2004-2005 1.2 million computer users suffered losses which added up to around $929 million
- U.S. businesses lose an estimated $2 billion per year as their clients become victims.

What are we doing about it?

- educating people about phishing to make them aware of possible attempts.
- Specialized spam filters
- Browsers alerting users of fraudulent sites.
- Augmenting password logins
- Anti Phishing Working Group

Legal responses.

In January 2007, Jeffrey Brett Goodin of California became the first defendant convicted by a jury under the provisions of the CAN-SPAM Act of 2003.

He was found guilty of sending thousands of emails to America Online users, posing as AOL's billing department, when open it prompted customers to submit personal and credit card information. He faced 101 years of possible jail time, however he was only sentenced to 70 months.

Ethical Issues

- There is no ethical use, the person phishing is trying to gather information in most cases to commit other crimes with that information.
- Always make sure you know where the emails you open come from.

Sources.

- http://technospecs.wordpress.com/2012/07/28/lawmakers-seek-to-criminalize-phishing/
- http://www.phishing.org/history-of-phishing/
- http://www.webopedia.com/TERM/P/phishing.html
- http://www.anti-abuse.org/phishing-general-information/
- http://www.itbusiness.ca/it/client/en/home/News.asp?id=67388&PageMem=2
- http://www.informationweek.com/california-man-gets-6-year-sentence-for/199903450
- http://www.queensu.ca/its/security/EducationAndAwareness/phishing.html

MONEY MULES.

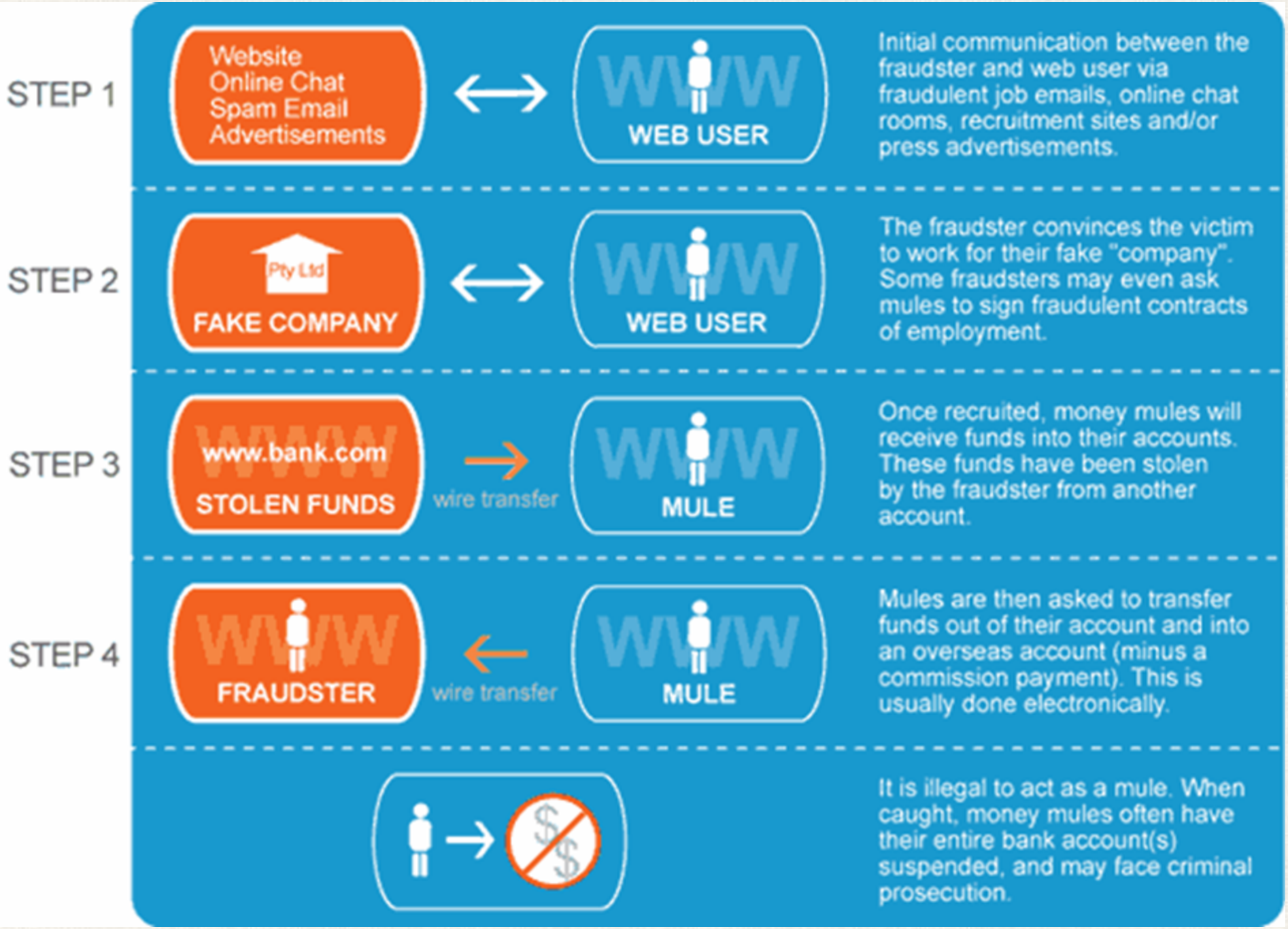
Jonathan Vaquera

What is a money mule?

- A person who transfers stolen money or goods between countries.
- Money mules aren't aware they are transferring illegal funds. They think they are just making transfers for a company.

Recruiting Money Mules

- Scammers typically post job offers through spam e-mails, letters by mail, newspapers, and internet chat rooms.
- Job titles usually include: payment processor, financial manager, and sales manager.
- Job description says you can make quick money. All you have to do is transfers for the company.


STEP 1
Website
Online Chat
Spam Email
Advertisements
WEB USER
Initial communication between the fraudster and web user via fraudulent job emails, online chat rooms, recruitment sites and/or press advertisements.
STEP 2
Pty Ltd
FAKE COMPANY
WEB USER
The fraudster convinces the victim to work for their fake "company". Some fraudsters may even ask mules to sign fraudulent contracts of employment.
STEP 3
www.bank.com
STOLEN FUNDS
wire transfer
MULE
Once recruited, money mules will receive funds into their accounts. These funds have been stolen by the fraudster from another account.
STEP 4
FRAUDSTER
wire transfer
MULE
Mules are then asked to transfer funds out of their account and into an overseas account (minus a commission payment). This is usually done electronically.
It is illegal to act as a mule. When caught, money mules often have their entire bank account(s) suspended, and may face criminal prosecution.

Where is the money coming from?

- Scammers will steal a victim's identity to gain access to their bank accounts.
- They withdraw anywhere from a couple thousand dollars, up to $100,000.
- Money may also come from human or drug trafficking.

Legal consequences.

- If you are caught transferring illegal funds, any of these things can occur:
  - Bank account will be frozen and/or closed
  - Any money you made will have to be returned
  - Credit/financial history will be ruined
  - You may required to pay back all the stolen money
  - Face jail time

Ethical Issues.

- The person who is caught, is unaware they were transferring illegal funds. So is it correct that they are charged for a crime they weren't aware they were committing?
- "Money mules are not accomplices, they are the true victims of theft fraud." - Cormach Herley and Dinel Florencio of Microsoft Research

Don't become a money mule.

- Pay attention to the job description.
- Never allow anyone you don't know transfer you money.
- Research the company who posted the job offer.
- If it sounds too good to be true, then it probably is!

Sources

- http://www.banksafeonline.org.uk/common-scams/money-mules/money-mules-explained
- http://news.softpedia.com/news/Money-Mule-Jobs-Masked-as-Mystery-Shopper-Offers-287078.shtml
- http://www.scambusters.org/moneymule.html
- http://threatpost.com/en_us/blogs/money-mules-not-customers-real-victims-bank-fraud-032712
- http://www.hotscams.com/articles/warning-fake-check-or-money-mule-scam.html
- http://www.afp.gov.au/policing/cybercrime/internet-fraud-and-scams.aspx

CORPORATE ESPIONAGE.

Terrance Williams

What is Espionage?

> the practice of spying to obtain information about the plans and activities, especially of a **foreign government** or a **competing company.**

$13 billion.


DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY

How did they do it *THEN?*

1990s - Mars vs Nestle.

Agents, working through subcontractors for Nestle, stole garbage bags from the Mars headquarters and replaced with with dummy trash bags looking for corporate records.

{ Candy Companies Mars and Nestle engaged in a corporate war through a confidential source nicknamed "Deep Chocolate." }

How do they do it *NOW?*

2010 - Operation Aurora.

Google discovered 'highly sophisticated and coordinated' cyber attacks originating from China that targeted over 20 companies. Google believed the Chinese government used the services to spy on human right activists.

{ The attacks used nearly a dozen pieces of malware and several levels of encryption to burrow deeply into the 'bowels of company networks' and obscure their activity. }

How do they do it *NOW?*

2011 - Operation Shady RAT.

Discovered by McAfee, over 70 corporations, governments, and nonprofit organizations were among those hacked in a five year hacking campaign that started in 2006 using a command-and-control server used by for directing the **r**emote **a**dministration **t**ools

{ United States, Canada, South Korea, and Taiwan as well as the UN, the International Olympic Committee, 12 defense contractors, and a South Korean construction company }

What are they after?

> According to the Economic Espionage Report from the Office of the National Counterintelligence Executive submitted to Congress, the following are the most targeted areas, primarily motivated by profit:

>> **Military** Technology
>> **Civilian** Technology
>> **Natural Resource** Supply and Location
>> **Communications** Technology


7:00 PM
Google
12.0MP
ZTE中兴


HUAWEI
HUAWEI
HUAWEI
HUAWEI

1985.

> ZTE was founded by 1985 by a group of state-owned companies affiliated with China's Ministry of Aerospace. It is the fifth largest telecom vendor in the world.

1988.

> Huawei was founded by Ren Zhengfei, a former engineer for the People's Liberation Army. It is the second largest telecom vendor in the world.

October 2012.

> After an 11 month investigation, U.S. House of Representatives' Intelligence Committee issues a report that accuses Huawei and ZTE for being arms of the Chinese government aiming to steal intellectual property from American companies and spy on U.S. citizens.

They recommended Huawei and ZTE be barred from supplying infrastructure to the US government and encouraged US corporations to do the same.

Ethical Considerations.

Previously, corporate espionage was largely a physical affair and a corporation's own employees were the largest source of espionage attacks.

In today's world, lines can be blurred between corporations and governments and the espionage itself is more advanced than ever. Because of this, security in the technology sector is more important than ever.

ID THEFT.

Thomas Wong

Identity Theft Basics.

- The illegal use of somebody else's personal information in order to obtain resources or credit in their name.
  - True Name
  - Account Takeover

Brief History.

- 1930s: ID theft was focused more on voting.
- 1964: The term "identity theft" was coined.
- 1930s - 1984: "Fake IDs" were used.
  - National Minimum Drinking Age Act
- 1998: Identity Theft and Assumption Deterrence Act of 1998 was passed.

How Is It Done?

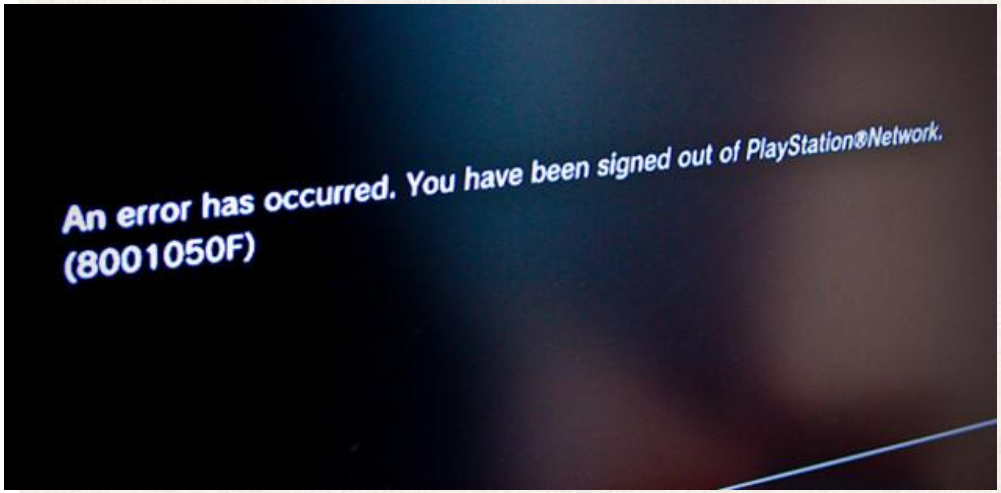
- Gathering Private Information
  - Database Hacking
  - "Skimming"
  - Dumpster Diving
  - Shoulder Surfing
  - Phishing
- Public Records
  - Grave Robbing
- Public Information

In 2000, 19% of all victims of identity theft had a personal relationship with the thief, and **10% of those were family members**. (FTC)

PlayStation Network Outage.

- April 17-19, 2011
- Over 2.2 million people had their personal information compromised.

PLAYSTATION®
Network



LifeLock.

- An identity-protection company based in Tempe, AZ.
- Charges $10/month for protection services.
- Guarantees $1 million in the event of an identity theft.

LifeLock Controversies.

- The CEO has had his identity stolen 13 times.
- The FTC sued LifeLock for $12 million.

Protecting Yourself.

Be Smart!

Ethical Considerations.

- Identity theft in any form is a crime.
- Using ID Protection Services
- You can never be too careful.

References

http://www.merriam-webster.com/dictionary/identity+theft
http://searchsecurity.techtarget.com/definition/identity-theft
http://money.howstuffworks.com/identity-theft2.htm
http://business.time.com/2012/04/24/grave-robbing-2-5-million-dead-people-get-their-identities-stolen-every-year/
http://news.cnet.com/8301-1009_3-20058513-83.html
http://en.wikipedia.org/wiki/PlayStation_Network_outage
http://en.wikipedia.org/wiki/LifeLock
http://www.wired.com/threatlevel/2010/05/lifelock-identity-theft/
http://www.wired.com/threatlevel/2010/03/lifelock-accused-of-running-con-operation/
http://money.howstuffworks.com/identity-theft3.htm

THE PATRIOT ACT.

Jeff Wells

USA Patriot Act.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

- Response to September 11, 2001
- Sunset December 2005
- Reauthorized by George Bush, Senate, House
- May 26, 2011 – Obama signed 4 year extension
  – Roving wiretaps, Business records

What is the Patriot Act?

Title I: Enhancing Domestic Security

Title II: Surveillance procedures

Title III: Anti-money-laundering to prevent terrorism

Title IV: Border Security

Title V: Removing obstacles to investigating terrorism

What is the Patriot Act?

Title VI: Victims and families of victims of terrorism

Title VII: Increased information sharing for critical infrastructure protection

Title VIII: Terrorism criminal law

Title IX: Improved Intelligence

Title X: Miscellaneous

Title II: Surveillance procedures.

- Trap & Trace surveillance
- Roving wiretaps
- Request communication records from providers: *Session times*, *IPs*, *addresses*
- Judge may request *ex parte*; no need to disclose reasoning
- Voicemail is normal warrant, not wiretap
- Enter and search property without owner's knowledge

Controversy.

Antoine Jones

– Linked to drug trafficking by unwarranted GPS on his car

Brandon Mayfield

– Incorrectly jailed for Madrid bombings after FBI raid and fabricated evidence

Ethical Questions.

Should the government be able to:

>> Tap our phones?

>> Search our homes without notifying us?

>> Track internet activity?

>> Spy on U.S. citizens?

Sources.

http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm
http://en.wikipedia.org/wiki/Patriot_act#Controversy
http://www.govtrack.us/congress/bills/107/hr3162/text
http://www.ord.uscourts.gov/rulings/04-cv-1427Opinion.pdf

ONLINE GAMBLING.

Matthew Tunnicliff

What is Online Gambling?

- Online gambling is simply gambling using the internet.
- It is also known as Internet Gambling or iGambling

Some History.

1994 - Antigua and Barbuda passed the 'Free Trade & Processing Act.'

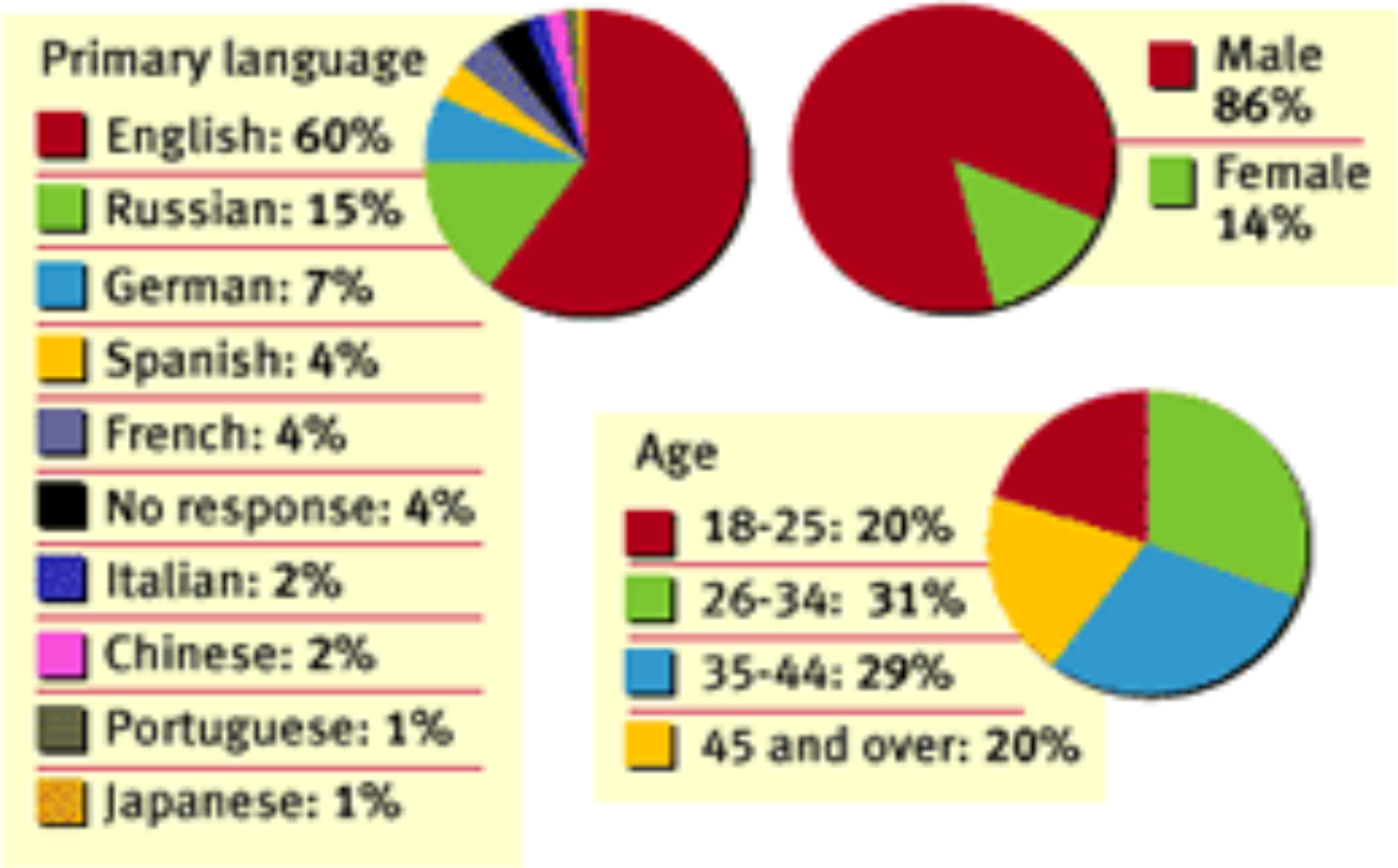
1999 - The 'Internet Gaming Prohibition Act' was introduced, but did not pass.

2000 - The 'Interactive Gambling Moratorium Act' passes in Australia, making all online casinos illegal unless they were created and licensed before May, 2000.

Growth.

- In 1996 there were 15 online gambling websites
- In 2004 there 44,000 websites
- In 2008 the online gambling revenue was about $21 billion.

WHO'S GAMBLING ONLINE?



SOURCE: Inland Entertainment Corp.survey of nearly 500 customers of kennyrogers.com, casinoaustralia.com and goodluck.com. The questionnaire was in English.

Types of Online Gambling.

- Sports Books
- Race Books
- Online Casinos
- Online Lotteries
- Bingo
- Electronic Stock Trading

INTERNET GAMBLING SITES

*EXCLUDING INSTANT BINGO, WHICH IS CATEGORIZED AS A SINGLE-PLAYER CASINO GAME.

** EXCLUDING INSTANT LOTTERIES, WHICH ARE CATEGORIZED AS SINGLE-PLAYER CASINO GAMES.

SOURCE: River City Group

Is Online Gambling Legal?

- It is not technically legal in the U.S., but it is hard to prosecute players.
- The Wire Act
- It is legal in around 70 countries including Australia, France, and Germany.

Ethical Considerations.

- Should we be able to gamble online if we can gamble in person?
- Websites can not tell a person's age, a underage person could gamble.
- It is easier to become addicted to online gambling.

Sources.

- http://en.wikipedia.org/wiki/Online_gambling
- http://entertainment.howstuffworks.com/online-gambling1.htm
- http://www.uri.edu/personal/awel5922/gambling.index.html
- http://definitions.uslegal.com/g/gambling/