Computer Guy Consulting
harryelver@gmail.com
520-990-4309

Cybersecurity Awareness
12-19-2022

Cybersecurity is up to you! Why do we have to be alert?

*(if you are a cpa firm)

IR 2018 245, December 7, 2018

The IRS reminds all professional tax preparers that they are required by federal law to create and maintain a written data security plan. Sole practitioners are just as vulnerable to data theft as practitioners in large firms.

The Gramm Leach Bliley Act of 1999 requires all financial institutions, which it also defines as professional tax preparers, to create and maintain information security plans. The Federal Trade Commission, not the IRS, administers this law and created a Safeguards Rule to administer it. Information about the FTC requirements can be found in IRS Publication 4557, Safeguarding Taxpayer Data.

Why do we have to be alert…..continued *(if you are a cpa firm)

FTC Safeguards Rule

Many companies collect personal information from their customers, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The Gramm Leach Bliley (GLB) Act requires companies defined under the law as “financial institutions” to ensure the security and confidentiality of this type of information. As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) issued the Safeguards Rule, which requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure.

WHY DOES CYBERSECURITY MATTER? FIGURES FROM MID-YEAR 2020

THE RISKS ARE REAL

Oh No, Look!

- "The worldwide information security market is forecast to reach $170.4 billion in 2022, according to Gartner. This is due in large part to organizations evolving their defenses against cyber threats — and a rise in such threats, including in their own companies.
- 95% of cybersecurity breaches are caused by human error. (Cybint)
- The worldwide information security market is forecast to reach $170.4 billion in 2022. (Gartner)
- 88% of organizations worldwide experienced spear phishing attempts in 2019. (Proofpoint)
- 68% of business leaders feel their cybersecurity risks are increasing. (Accenture)
- On average, only 5% of companies' folders are properly protected. (Varonis)
- Data breaches exposed 36 billion records in the first half of 2020. (RiskBased)
- 86% of breaches were financially motivated and 10% were motivated by espionage. (Verizon)
- 45% of breaches featured hacking, 17% involved malware and 22% involved phishing. (Verizon)
- An estimated 300 billion passwords are used by humans and machines worldwide. (Cybersecurity Media)

HORNE CYBER

4

hornecyber.com

HORNE CYBER

Cyber Fraud is Growing (Internet Crime Complaint Center)

https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

What??? Some definitions would be helpful.

Phishing: the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. "an email that is likely a phishing scam"

Vishing: the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers. "many victims of vishing are people who are not tech-savvy"

Smishing: the fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers. "police say they have busted a gang in Maitland suspected of smishing"

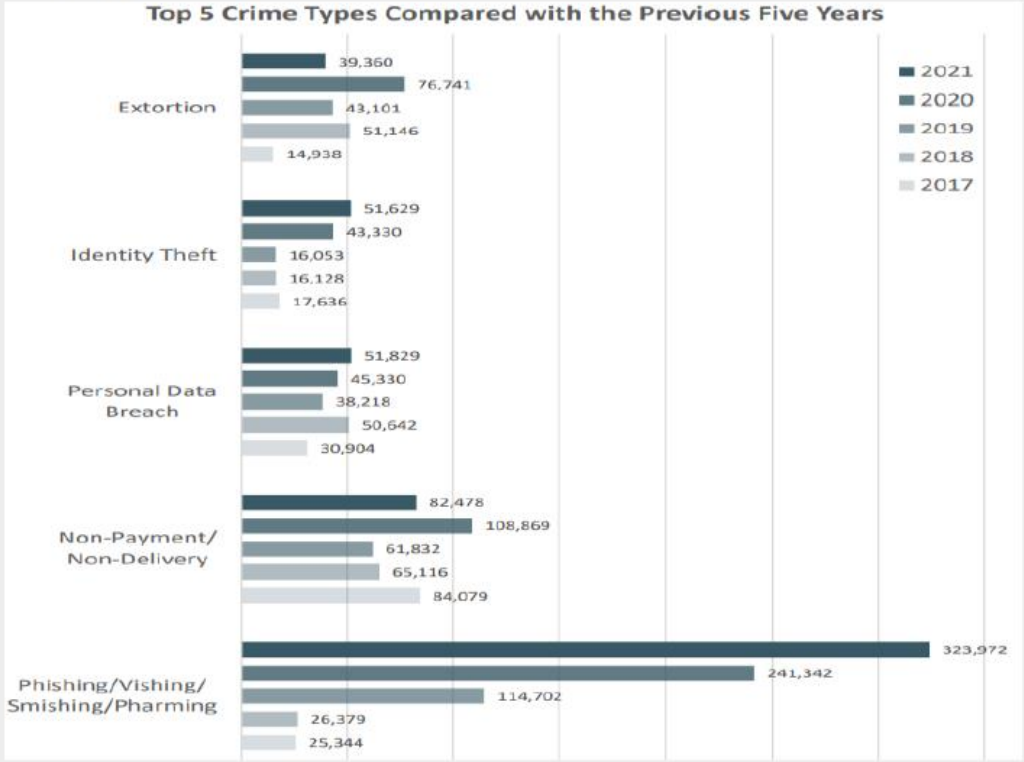
Pharming: is a cyber attack intended to redirect a website's traffic to another, fake site by installing a malicious program on the computer.

BEC: Business email compromise (BEC)—also known as email account compromise (EAC)—is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business—both personal and professional.

Malware: software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Ransomware: a type of malicious software designed to block access to a computer system until a sum of money is paid.

IC3 Complaint Statistics (Internet Crime Complaint Center)



https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

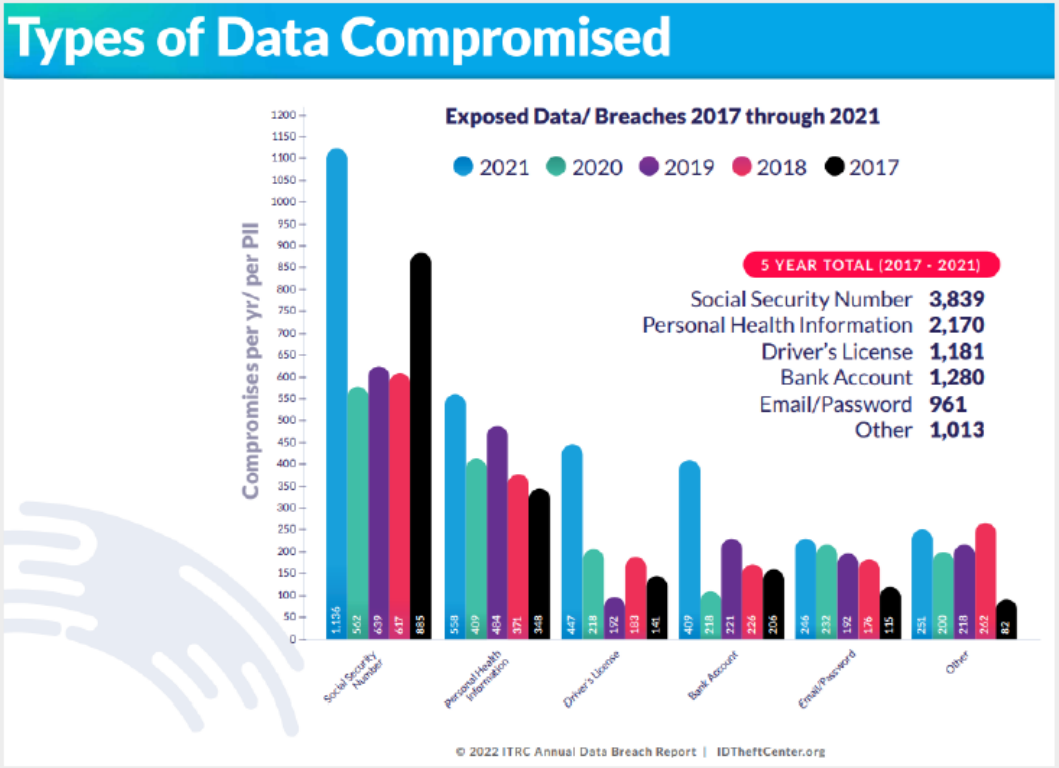
Data Breaches

The release or taking of data from a secure source to an unsecured third-party location (Computer).

Data Breaches (Identity Theft Resource Center)

http://www.idtheftcenter.org/

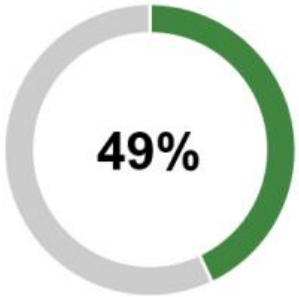
Data Breaches



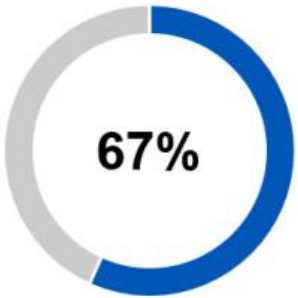
http://www.idtheftcenter.org/

WHY ARE USERS THE WEAKEST LINK?

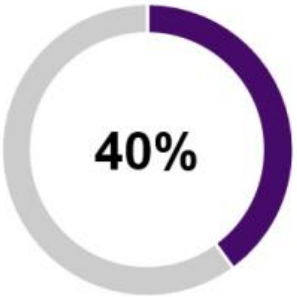
of workers who know they've been hacked don't bother to change their passwords afterward[1]



of employees admit they click links in messages from unknown senders during work[1]



of workers are sure they've received at least one phishing email at work[1]



Of those who received a phishing email, ~40% didn't report it

HORNE CYBER

ALMOST GUARANTEED ACCESS TO OUR NETWORKS

- Phishing
  - Email address spoofing (ex: lmge.com)
  - Targeted, using publicly available information to seem legitimate
  - Malicious links in email body or in attachments
- Pretexting
  - Call masquerading as IT support or customer/vendor
- Baiting
  - Thumb drive on ground
- Physical access
  - IT/Phone/internet provider impersonation

HORNE CYBER

Oh Harry, What can we do?????

Pandora's Box

Use Common Sense

You wouldn't leave your personal items unattended in a busy airport or let a stranger borrow your car, because that wouldn't be logical or safe.

Never give confidential information to anyone over the phone, through email, ~~on social media~~, or via text message unless you can verify that they are legitimate and trustworthy.

IT'S SAFE ONLINE, RIGHT?

1 in 50 URLs is malicious[1]

Nearly 1 in 3 phishing sites uses HTTPS to appear legitimate[1]

90% of the malware businesses encounter is delivered via email[2]

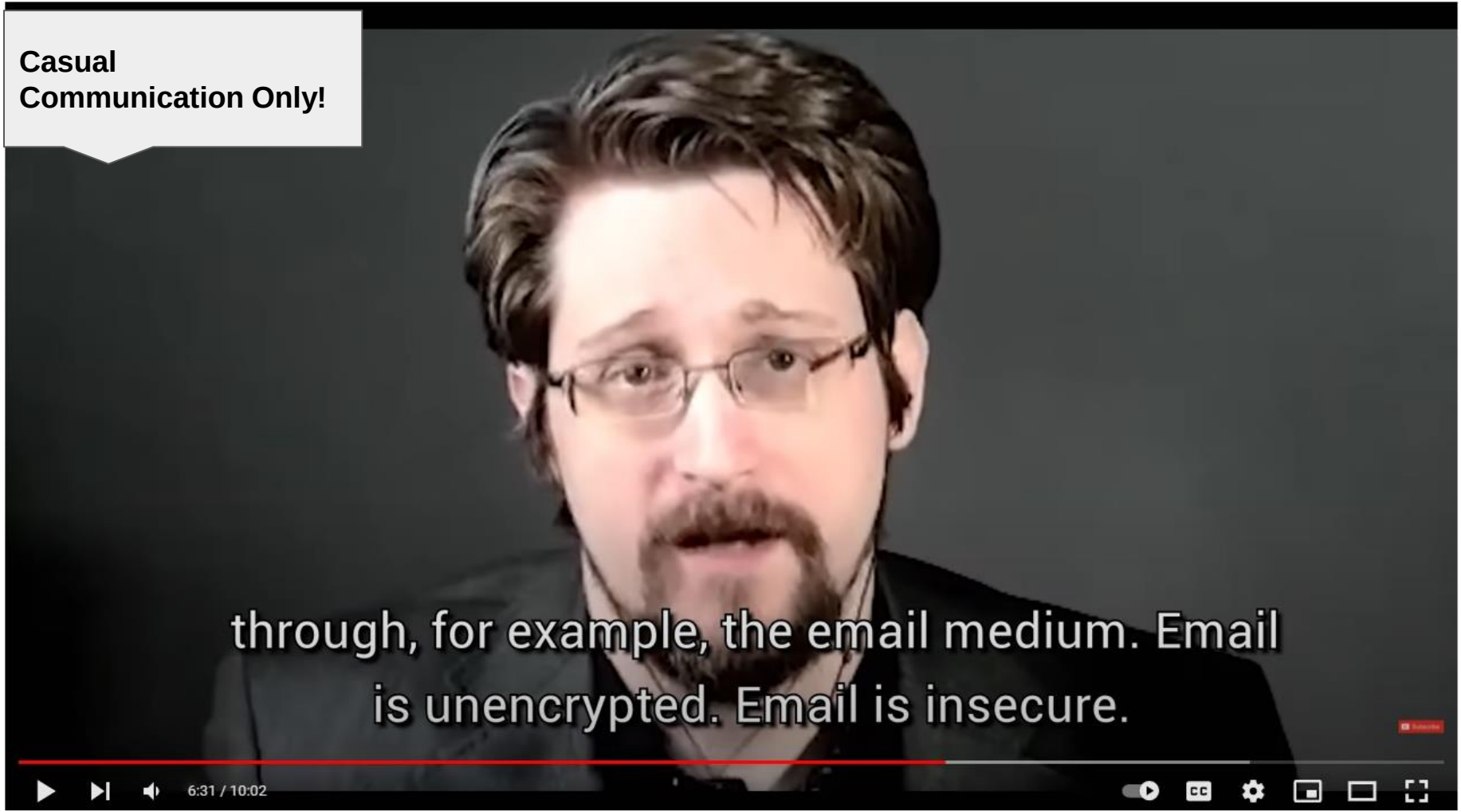
Most breaches involve phishing and using stolen credentials[2]

[1] Webroot Inc. "2019 Webroot Threat Report: Mid-Year Update." (September 2019). [2] Verizon. "2019 Data Breach Investigations Report." (May 2019)

HORNE CYBER

No it's not safe, be careful!!

Casual Communication Only!



Risks

Card data is also at risk when being transferred or transmitted.
You should assume that NONE of these are secure, particularly when it comes to sending ANY card data, and never transmit unencrypted data this way.

…….Credit Cards……

Be Aware of the PII You're Trusted With

The key word in that statement is "trust."

Everyone we work with trusts us with sensitive data.

You can accomplish these goals:

By staying alert at all times

By never making assumptions

By thinking before clicking

Key Takeaways:

- Social engineering is the art of manipulating people, not computers.

- These attacks utilize a variety of mediums including email, text messages, and phone calls.

- Never reveal confidential information unless you can confirm the recipient is legitimate.

Can prevent a data breach!

Please complete the cyber training at knowbe4.com. (yes, there was an email)

Contact me when in doubt:

Desperate: call me 520-990-4309

Less Desperate: text me 520-990-4309

Ain’t no biggie: email harryelver@gmail.com