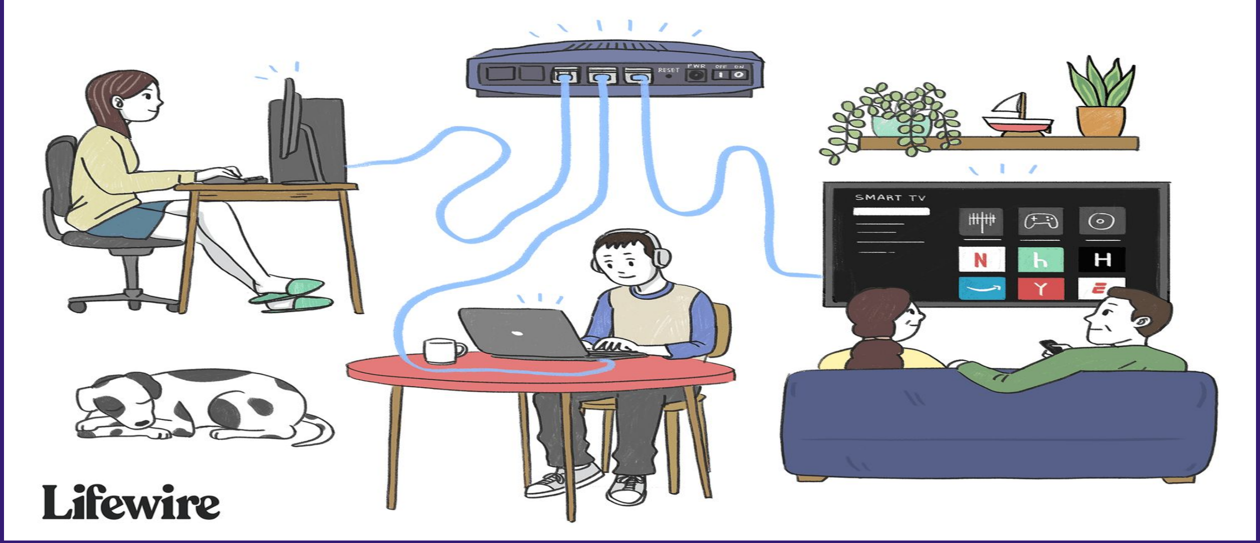
Online Financial Safety

Austin Davis, Dennis Skoy, Lucy Eldredge, Matthew Jensen, Mausham Bista

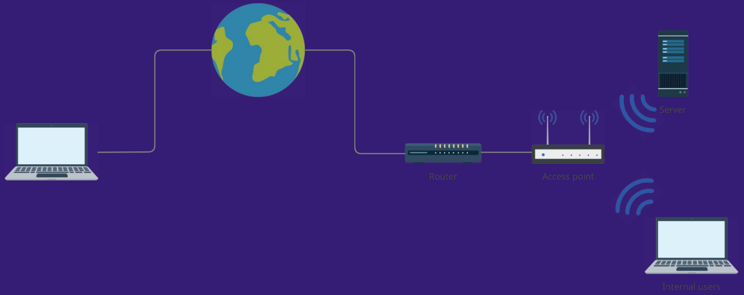
Network



A system connecting devices to one another within a given location

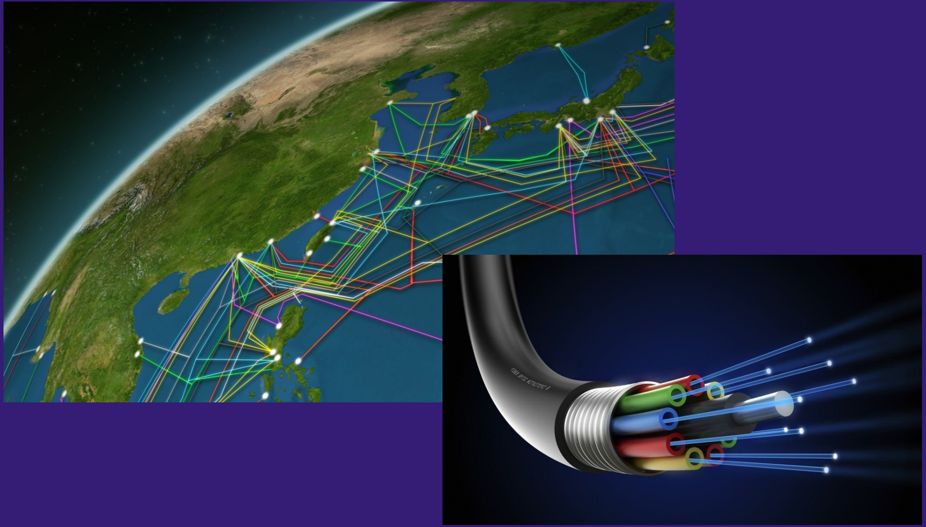
- LAN (Local Area Network)
  - Most common type used
    - Found in households and small businesses.

Internet



A global system of cables connecting networks throughout the world

The internet connects you to another network, accessing that data from any location



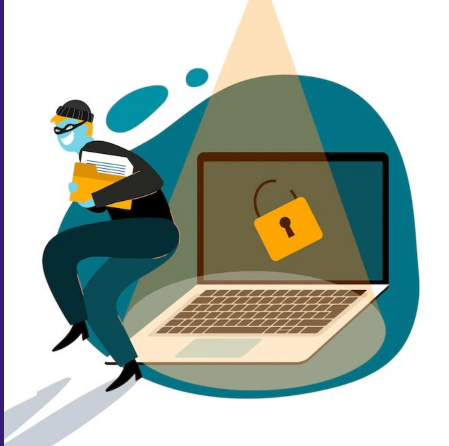
This provides:

- universal access to information
- global communication
- convenient connections to goods and services

Online Banking Services

The internet enables banks to provide remote account access for their customers

- Instant monetary transactions
- Account management from afar
- Reducing needs to visit your local bank for adjustments or services



Threat Actor

Threat actors are individuals attacking your data security

- Forcing your devices (tablets, phones, computers, etc) to malfunction or break
- Stealing your personal information
- Accessing your bank accounts and finances

Threat Actor Motives

Financial gain

- Extort money from individuals, businesses, and governments

Political/Ideological

- Disrupt businesses or government functions

Notoriety/Leisure

- Out for revenge
- Doing it for fun

Threat Actor Attacks

Credit Card Fraud

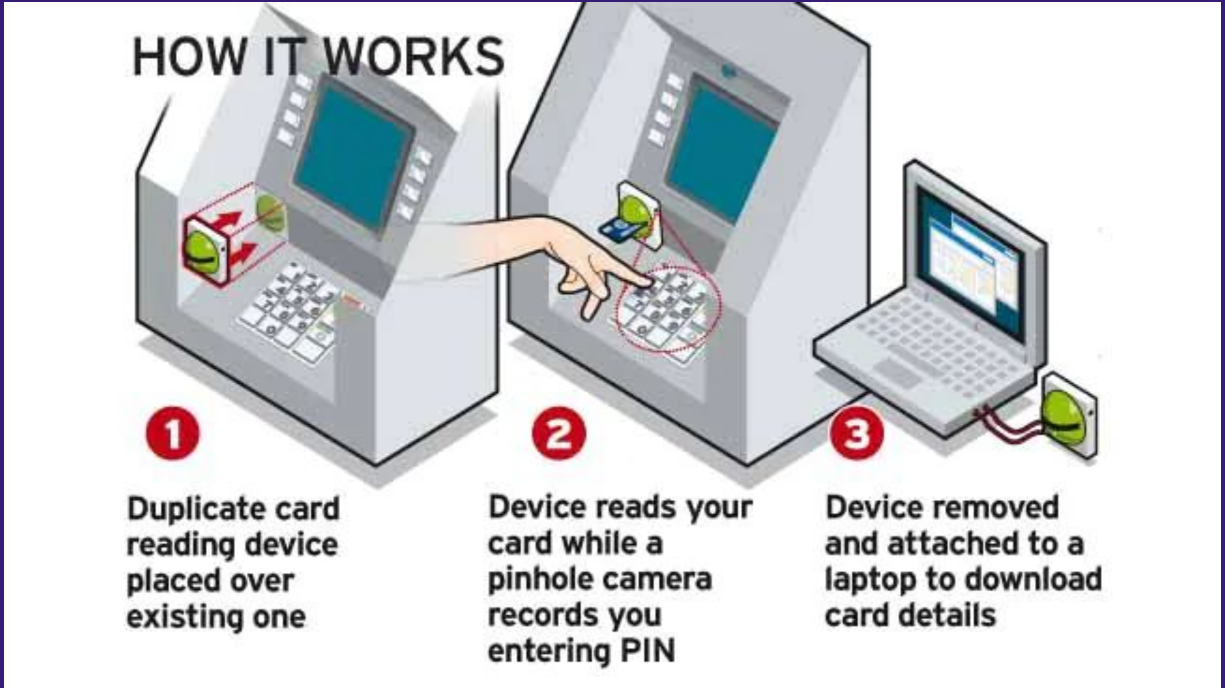
Credit card information is stolen to make purchases

- Charging personal accounts
- Damaging finances
- Impacting credit

Threat Actor Attacks

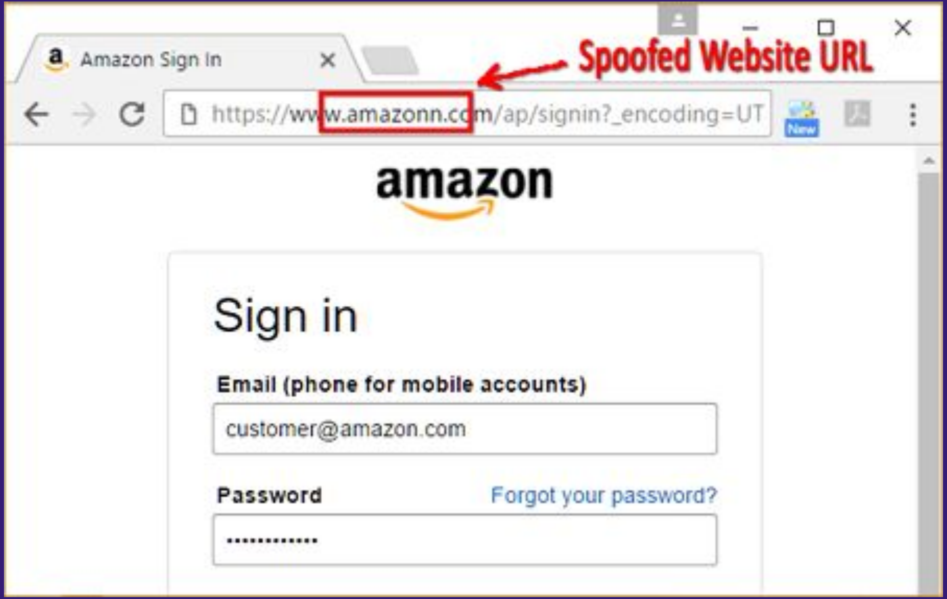
Credit Card Fraud: Skimming

Threat actors placing a device on card readers to scan and save debit/credit card information


HOW IT WORKS
1
Duplicate card reading device placed over existing one
2
Device reads your card while a pinhole camera records you entering PIN
3
Device removed and attached to a laptop to download card details

Threat Actor Attacks

Site Spoofing



Sign in

Email (phone for mobile accounts)

customer@amazon.com

Password

·············

A Threat Actor creates an identical website to a legitimate website

- pretends to be that company
- steals sensitive information when people don’t notice the difference
- uses that sensitive information to access personal accounts

Threat Actor Attacks

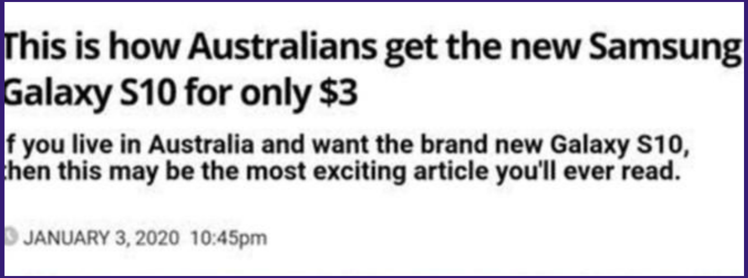
Social Engineering

Exploiting and manipulating human flaws to access personal information and protected systems

Hacking human psychology instead of computers

Threat Actor Attacks

Social Engineering Attacks



This is how Australians get the new Samsung Galaxy S10 for only $3

f you live in Australia and want the brand new Galaxy S10, hen this may be the most exciting article you'll ever read.

JANUARY 3, 2020 10:45pm

Phishing : texts/emails requiring your input, impersonating a financial institution, government authority, or business

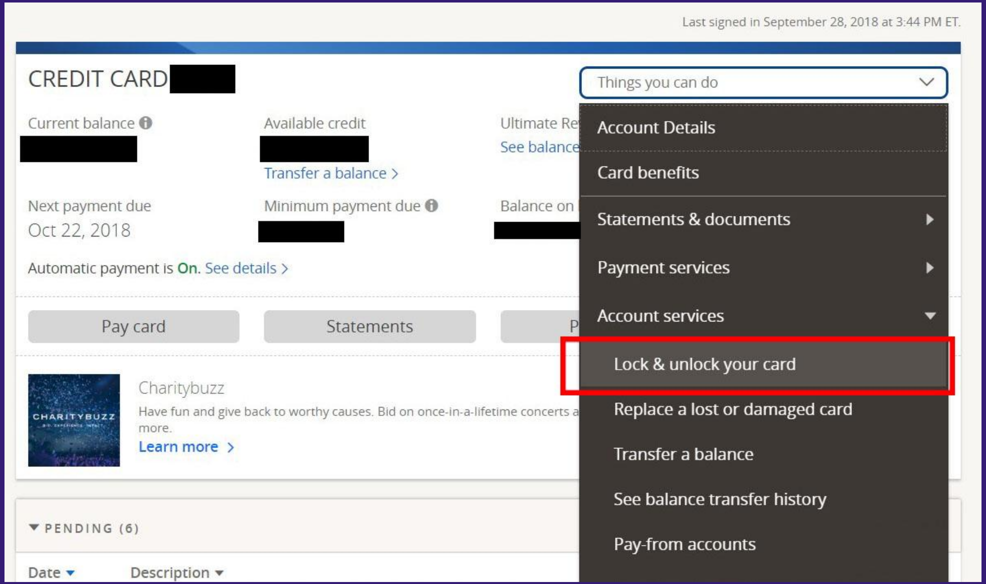
- Provides a direct link
    - Clicking corrupts your device

Physical Interaction : exploiting human sympathy/trust to bypass authority and access private accounts/locations

Source: https://www.investopedia.com/terms/s/social-engineering.asp#:~:text=expert%20and%20educator.-,What%20Is%20Social%20Engineering%3F,to%20penetrate%20a%20target%27s%20account.

Financial Protections

Debit/Credit Card



Last signed in September 28, 2018 at 3:44 PM ET.

CREDIT CARD [redacted]

Current balance [redacted]

Available credit [redacted]

Ultimate Re

Next payment due Oct 22, 2018

Minimum payment due [redacted]

Balance on [redacted]

Automatic payment is On. See details >

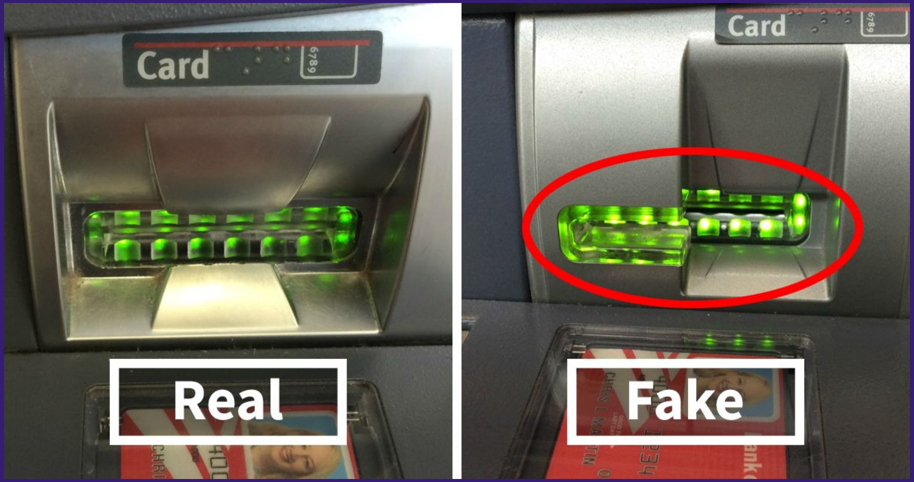
Charitybuzz

Have fun and give back to worthy causes. Bid on once-in-a-lifetime concerts a more.

- Report any odd or suspicious transactions that you didn’t authorize on your card
- Do not save your credit/debit card information on websites
- Locking your credit/debit card prevents threat actors from misusing it
- Contact your banking provider to lock any lost or stolen debit/credit cards ASAP

Protections

Watch for Skimming Devices



Check for fake card readers before using the device

- bulky/loose fitting attachments on the PIN keypad

Report this device to your local law enforcement if found

Protections

Log Out Accounts/Shut Off Computers

Log out of all accounts or devices you are done using

- Prevents threat actors from stealing information from that account/device
- Stops account and device misuse from family, work associates, and strangers

Protections

Implement Two Factor Authentication

PASSWORD
Username
****
Login
VERIFY

Requires individuals to verify that they are the person logging in

- Requiring your permission every time you log in

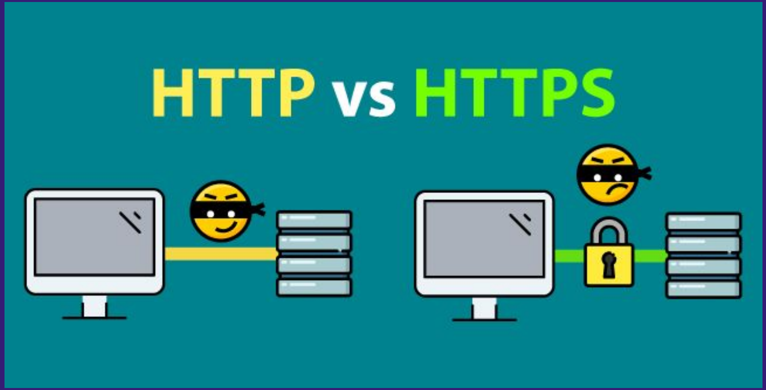
Ex. Receiving a request on their phone to verify their identity

Protections

Online Account Protection

Change your Passwords frequently

- changing/rotating passwords keeps threat actors with old information out of your accounts
- Keep and update your new passwords in a safe location or password manager

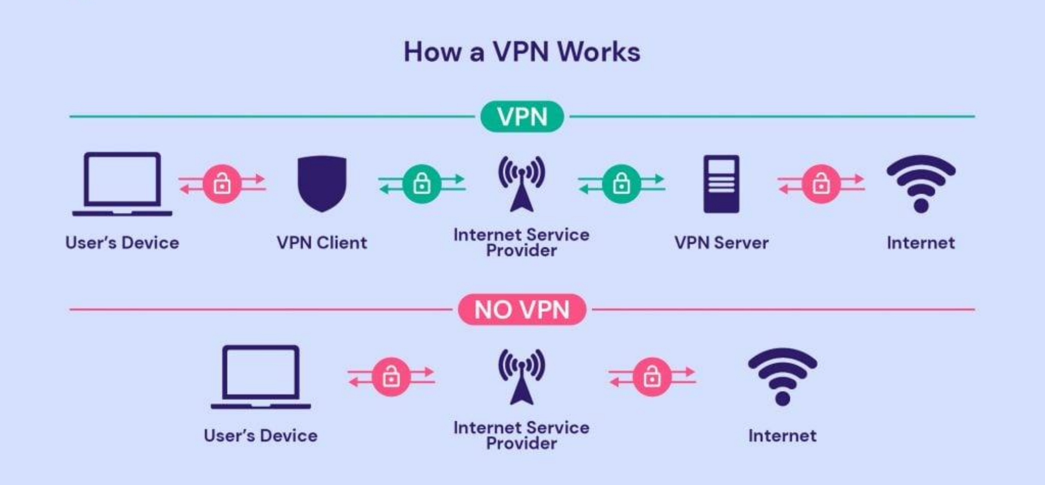


Connect to the Internet Securely

- Check the website’s URL for a lock symbol
- Ensure the start of the url says HTTPS.
  - If the url says and HTTP (not HTTPS) it is not secure.

Protections

Use a VPN on Public Wifi



Easily to Access = Easy to Exploit

Use a VPN when connecting to wifi in a public place, hotel or airport

- hides your internet usage from internet provider
- protects your important accounts and credentials that require an online connection

Protections

Fake Urgency/Authority

Don't provide personal or financial information to sudden messages

- Legitimate organizations do not request:
  - your social security number
  - banking account number
  - credit card number

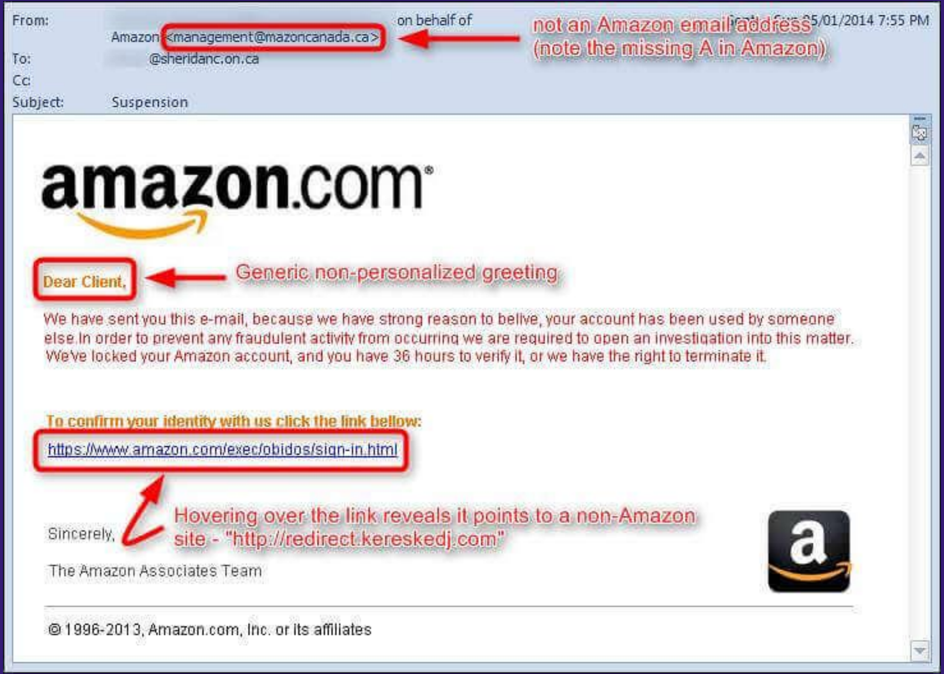
Avoid immediate action

- Scammers pressure individuals to pay or provide information
- Certified organizations proved enough time to make informed decision

Source : https://consumer.ftc.gov/articles/how-avoid-scam

Protections

Links and Attachments



From: [redacted] on behalf of Amazon <management@mazoncanada.ca> 05/01/2014 7:55 PM
To: [redacted]@sheridanc.on.ca
Cc:
Subject: Suspension

not an Amazon email address (note the missing A in Amazon)

amazon.com

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:
https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates

Check for hazardous links and attachments

- Only open files you know are safe
- Hover the mouse over a link to see where it will take you

Source: https://www.arcsystems.co.uk/the-dangers-of-links-and-attachments-in-emails/