HIGHTOWER

Protect Yourself from Cybercrime

With cybercrime activity so prevalent in the world today,[1] it is a good time to review what it is and how to avoid it. Whether you're using a desktop or mobile device (such as a smartphone, tablet, laptop, smart watch, handheld gaming console, or e-reader), precautions need to be taken to avoid loss of your identity and your money.

Common Scenarios of Fraud, Scamming, Phishing and Hacking

Though methods vary, all cybercrimes have a common origin: personal information is shared (either intentionally or unintentionally) with an unknown person or entity over the phone, on a computer, or through a mobile device. Here are a few examples of different types of cybercrime.

01

An individual masquerading as a process server, law enforcement officer, debt collector or attorney

What may occur:

- A process server or attorney contacts a person by phone with notification of legal action being taken against them.
- To release court documents, or pay court fees, you will be asked to pay costs over the phone.
- A debt collector or law enforcement officer insists you have delinquent, unpaid debt and demands payment.

02

Scammers impersonating Best Buy's Geek Squad[2]

What may occur:

- You receive a fake invoice from the Geek Squad's "auto-renewal" service. To block the auto-renewal, customers are directed to call a fraudulent phone number.
- You receive a call from a Geek Squad member asking for personal information (name, address, date of birth, Social Security number, driver's license number, and more).
- Thieves will likely ask for remote access to your computer to rapidly steal your banking or financial institution information and drain money from your accounts.

03

Phishing bait: clicking on buttons or links within an email or text message

What may occur:

- You'll receive an email from an individual posing as a friend or co-worker with a link or downloadable attachment that will allow them to gain access to your account or computer.
- Hackers, disguised as a seemingly reputable organization, such as your bank, utility company, the IRS, etc., will send you an email with a downloadable attachment or link.
  - A request may be disguised as a link or button that sends you to a fraudulent web page to verify your account details.
- Watch out for package tracking scams via text or email.
  - These messages usually contain a tracking link with prompts to update your delivery.

04

Social media phishing

What may occur:

- Hackers gain access to social media accounts and impersonate you with posts or send requests or emails to friends and family with fake pleas for help or money.
- Be wary of online quizzes on social media that collect personal details. You may be prompted to answer seemingly innocuous questions, such as:
  - How many states have you traveled to?
  - What makes and models of cars have you have owned?
  - What Marvel character would you be?
  - What are your favorite foods?
  - What are your grandchildren's names?
  - Where did you meet your spouse?
  - What is your pet's name?
- Sure, those social media quizzes are fun, but scammers on the dark web can use your answers to reset your account logins, guess passwords, and access your accounts - all leading to identity and financial theft.[3]

These Red Flags Can Alert You to Cybercrime

By no means a comprehensive list, these activities are tip-offs that something is a potential scam or crime:[4]

- Requests to provide your personal information: name, address, account numbers, driver's license number, SSN, credit card numbers, date of birth, family member contact and personal information.
- Suspicious emails with email attachments, downloading files from suspicious websites.
- Demand for immediate payment, or for payment via a gift card, wire transfer, or prepaid debit card. All are difficult to trace.
- A phone call, text or email claiming unpaid debt you don't recognize.
- You're prevented from logging into your email or social media account.
- Your Email Sent folder has messages you didn't send or has been emptied.
- You're notified by friends, family, or on social media that you're being impersonated.
- You've received a call from a "grandchild" or other family member saying they're in trouble and need money immediately.
- Threats and Pressure:
  - You're in trouble with the government
  - You owe money, someone in your family has an emergency
  - Do not hang up
  - You will be arrested
  - Your computer is corrupted
  - Your grandchild is in trouble
  - You have a computer virus
  - You've won a lottery or sweepstakes
  - Call law enforcement or we will have you arrested requests with an unusual sense of urgency
- Your security software has been:
  - Disabled or compromised
  - Computer speed has slowed down significantly
  - No access to accounts
  - Random shutdowns and restarts
  - Mismatched information
  - Unprofessional communication

Remember: anything that's too good to be true, usually is.

Ways to Avoid a Scam or Hack[5]

- Never give personal information in response to a request you did not expect or make.
- Pause, think and research – Hang up and call someone you trust to explain the situation.
- Look for the lock:
  - When online, look for a locked padlock in the address bar of your web browser and "https", not "http", indicating the connection is secured and encrypted.
- Remember a professional process server or attorney will never ask for money, ask for your SSN, or threaten to call the police for non-payment or to release court documents.
- A debt collector will always provide their name, company, address, phone number and a professional license number.
  - Insist on identification from the caller.
- Never pay anyone who insists on payment in cryptocurrency, a wire service such as Western Union or a gift card.
- Never deposit a check and mail the money back to an unknown party.
- Check on your family members (especially grandchildren) - are they really in trouble?
- Beware of fake texts as hackers will attempt to engage with you through your mobile devices.
  - Stay vigilant to recognize changes in text style or links to request a different method of communication.
- Block unwanted calls or texts on your mobile or home phone.

Next Steps

Everyday hackers, scammers and those operating unethically, are developing sophisticated methods of taking advantage of consumers. Should this happen to you, call someone you trust, explain the situation, and ask for help. Taking immediate action will make the difference between protective action and loss.

- Should a cyberattack happen to you or someone you know, you can take the following steps:[6]
  - Contact the police
  - Contact the fraud department of each of your creditors
  - Complete a Federal Trade Commission (FTC) Identity Theft Affidavit
  - Contact your banks or financial institutions
  - Report the incident to the fraud department of the three major credit bureaus[7]

EQUIFAX

To report fraud: 1-800-525-6285
To order a credit report: 1-800-685-1111
TDD: 800-255-0056
www.equifax.com

EXPERIAN

To report fraud: 1-888-397-3742
To order a credit report: 1-888-397-3742
TDD: 800-972-0322
www.experian.com

TRANSUNION

To report fraud: 1-800-680-7289
To order a credit report: 1-800-888-4213
www.transunion.com

ADDITIONAL RESOURCES	"7 Practices to Protect Against Cyber Crime" READ	"What to Trust" WATCH

HIGHTOWER

200 W MADISON, 25TH FLOOR
CHICAGO, IL 60606
(312) 962-3800
HIGHTOWERADVISORS.COM

[1] https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=390346a519db
[2] https://wjla.com/news/local/scammers-impersonating-best-buy-geek-squad-fake-invoices-fake-renewal-notices-federal-trade-commission-ftc-warning-how-to-avoid-scam-alert-customers-steal-money-banking-information-emails-links-call-for-action
[3] https://consumer.ftc.gov/consumer-alerts/2023/01/dont-answer-another-online-quiz-question-until-you-read
[4] https://consumer.ftc.gov/articles/how-avoid-scam#signs
[5] http://myfloridalegal.com/pages.nsf/Main/957A7C53EE0E961E85257F77004BE172
[6] https://consumer.ftc.gov/articles/how-recover-your-hacked-email-or-social-media-account
[7] http://myfloridalegal.com/pages.nsf/Main/957A7C53EE0E961E85257F77004BE172