Are you about to cash a check from an item you sold on the Internet, such as a car, boat, jewelry, etc?

- Is it the result of communicating with someone by email?
- Did it arrive via an overnight delivery service?
- Is it from a business or individual account that is different from the person buying your item or product?
- Is the amount for more than the item’s selling price?

Are you sending money overseas?

- Did you win an international lottery you didn’t enter?
- Have you been asked to pay money to receive an inheritance from another country?
- Are you receiving a commission for accepting money transfers through your bank and/or PayPal account?

To report an online crime, go to: www.IC3.gov

DON’T BE A VICTIM OF IDENTITY THEFT!
The IC3 participates in multiple initiatives targeting an array of cyber crime schemes that victimize individuals and businesses domestically and abroad. These initiatives are a coordination of industry resources along with the investigative resources provided by cyber crime task forces comprised of federal, state, and local law enforcement agencies. The success of these initiatives is directly attributable to the inclusion of the industry resources. Initiatives focus on the following:

Charitable Contributions Fraud
Counterfeit Check Fraud
Identity Theft Task Force
International Fraud
Investment Fraud
Online Pharmaceutical Fraud
Phishing
Work-at-home scams

2014 IC3 Statistics:
3,175,611 Complaints Reported to IC3 Since Inception

www.ic3.gov
Mission of the IC3:
The mission of the Internet Crime Complaint Center (IC3) is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with industry partners. Information is processed for investigative and intelligence purposes for law enforcement and public awareness.

The IC3 Alliances:
The IC3 Unit is part of the Cyber Division’s Cyber Operations Section V within the FBI. The IC3 Unit is staffed by FBI agents and professional staff employees with expertise in the prevention, detection, and investigation of cyber crime.

The IC3 has formed additional alliances with industry representatives (e.g. online retailers, financial institutions, Internet service providers, and parcel delivery providers) that have exponentially increased the flow of the IC3’s most valuable commodity - INFORMATION. Working with federal, state, local, and international law enforcement, as well as regulatory agencies, IC3 analysts receive, develop, and subsequently refer information for investigative and prosecutive attention.

Cyber Crime and the IC3:
As technology evolves, so do the many methods used to exploit technology for criminal purposes. Nearly all crime that once was committed in person, by mail, or over the telephone can be committed over the Internet. The criminal element is empowered by the perceived anonymity of the Internet and the ease of access to potential victims. Criminals use social engineering to prey on their victims' sympathy, generosity, or vulnerability. The IC3 was designed to help address all types of cyber crime through its complaint system.

IC3 Complaints:
The complaints submitted to the IC3 cover an array of cyber crime including theft of intellectual property rights, computer intrusion, economic espionage, online extortion, and international money laundering. Numerous fraud schemes such as identity theft, phishing, spam, reshipping, auction fraud, payment fraud, counterfeit goods, romance scams, and non-delivery of goods are reported to the IC3.

Searching the IC3 Database:
The IC3 recently expanded the remote search capabilities of the IC3 database making it available to all sworn law enforcement and FBI personnel through the Law Enforcement Enterprise Portal (LEEP). Users can connect directly to the IC3 Complaint Search after authenticating through LEEP from the user’s Identity Provider (IDP) or through the user’s Law Enforcement Online membership at www.leo.gov. Users may also contact the IC3 for analytical assistance. While developing a case in the database, Management and Program Analysts compile similar complaints, collect relevant case information from both open-and-closed source public information databases and confer with federal, state, local and international law enforcement personnel. The IC3 compiles this information into reports that are available to all law enforcement.

Public Service Announcements:
The IC3 prepares public service announcements on the latest cyber trends to alert consumers on Internet fraud. These announcements are posted on the following Web sites:

www.ic3.gov
www.fbi.gov
Ransomware is a form of malware that targets both human and technical weaknesses in organizations and individual networks in an effort to deny the availability of critical data and systems. Ransomware is frequently delivered through spear phishing e-mails to end users. When the victim organization determines they are no longer able to access their data, the cyber actor demands the payment of a ransom, at which time the actor will purportedly provide an avenue to the victim to regain access to their data. Recent iterations target enterprise end users, making awareness and training a critical preventative measure.
Key areas to focus on with ransomware are prevention, business continuity, and remediation. As ransomware techniques continue to evolve and become more sophisticated, even with the most robust prevention controls in place, there is no guarantee against exploitation. This makes contingency and remediation planning crucial to business recovery and continuity.

Prevention Considerations

- Implement an awareness and training program. Because end users are targeted, employees and individuals should be made aware of the threat of ransomware and how it is delivered.
- Patch operating systems, software, and firmware on devices, which may be made easier through a centralized patch management system.
- Ensure anti-virus and anti-malware solutions are set to automatically update and that regular scans are conducted.
- Manage the use of privileged accounts. Implement the principle of least privilege: no users should be assigned administrative access unless absolutely needed; those with a need for administrator accounts should only use them when necessary.
- Configure access controls, including file, directory, and network share permissions, with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

Business Continuity Considerations

- Back up data regularly, and regularly verify the integrity of those backups.
- Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Examples might be securing backups in the cloud or physically storing offline. Some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real time, also known as persistent synchronization. Backups are critical in ransomware; if you are infected, this may be the best way to recover your critical data.

Other Considerations

- Implement application whitelisting; only allow systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value, and implement physical/logical separation of networks and data for different organizational units.

The Ransom

The FBI does not support paying a ransom to the adversary. Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom. Paying a ransom emboldens the adversary to target other organizations for profit, and provides for a lucrative environment for other criminals to become involved. While the FBI does not support paying a ransom, there is an understanding that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

In all cases the FBI encourages organizations to contact a local FBI field office immediately to report a ransomware event and request assistance. Victims are also encouraged to report cyber incidents to the FBI’s Internet Crime Complaint Center (www.ic3.gov).