

RECOGNIZING AND COMBATING CYBER-CRIME AND CYBER-STALKING

CYBER-CRIME

Cyber-crime is rampant on the Internet now and has been for several years. From identity theft to cyber-stalking to financial exploitation, criminals around the world are actively committing crimes using the Internet. While their methods are many, the end goal is almost always to make money, whether that is through stolen identities, get-rich-quick scams, tax fraud, extortion, or illicit trade.

Here are some common identifiers of scams and fraud perpetrated through email:

1. The subject line will address you by your email address, not your name. A lot of simple email scams use large lists of email addresses, with little or no accompanying information. Therefore, when “Wal-Mart”, or “CVS”, or even the “IRS” send an email and don’t use your real name in the subject line, you can usually assume it is a scam.
2. The email will create an immediate sense of urgency with phrases like “we have been trying to reach you”, “you must reply immediately”, or it may threaten you with fines, penalties or even jail time if you do not respond. Legitimate businesses and government agencies will contact you via other methods if they really need to do so.
3. There will be many examples of poor grammar, misspelled words, missing punctuation, incorrect use of capital letters, odd formatting or stilted expressions like “we apologies for any inconvenience” or “send me a message immediately payment is completed”.
4. The email will purport to be from “Administration” or “Service Desk” or other some authoritative source, but will show as having come from a completely different email address. For example, here at Berry, you should never get an email about grades, tuition payments, work or payroll that doesn’t come from the @berry.edu domain.
5. If it seems too good to be true, it most likely is. Receiving an email from the estate of a relative you have never heard of who has left you thousands of dollars in their will, or from someone you don’t know (usually in another country) who needs help transferring or disposing of huge sums of money just doesn’t happen.

Scammers play on your emotions by tapping into your greed, your forgetfulness, your fear, your loneliness, and your kindness. [This article](#) has a number of examples of these types of emails.

CYBER-STALKING

Crime doesn’t always have a monetary goal. Sometimes the goal is to intimidate, terrorize, or exert undue pressure on another person. While not all instances of cyber-stalking reach criminal levels, every instance can

be very intrusive and demeaning to the intended victim. Social media, in all of its forms, is a perfect weapon to wield in this kind of crime. Here are a few ways to spot and avoid cyber-stalkers.

1. Cyber-stalkers will generally “groom” their targets in various ways. Be cautious of people who seem overly interested in you, especially those that request personal details of any kind.
2. Be cautious about accepting social media requests from people you don’t know. Period. At the very least, check out their profile. If it is short on details, it is a good sign they are not who they claim to be or are hiding something. Also, if they seem to have only one type of friend, i.e. college age females or college age males, especially with no family listed, be very cautious.
3. Be wary of people who excessively flatter, this is a sign that they may be attempting to “groom” you as a target.
4. Never give out personal information to online friends you don’t know “in the real world”, as they can then use this information to physically stalk you.

Serious cases of cyber-stalking should be reported. [The Berry College Police](#) should be the first department to contact unless the cyber-stalking has an aspect of sexual misconduct, i.e., the stalker has expressed a sexual interest in their victim or has included lewd and suggestive language in their communications. In this case students should contact a Title IX officer, all of which are listed [on this page](#) on the college website, and report the stalking.

While the Internet is a great place to share stories with friends, hang out, learn, and be entertained, unfortunately there are plenty of people out there who want nothing more than to take advantage of others, whether by stealing from them financially through scams or by stealing from them emotionally through cyber-stalking. Being aware of how these criminals operate is an important step toward being safe. Here are a couple of resources with more details about cyber-stalking and how to avoid it.

NoBullying.com - [Learn How to Deal With a Stalker](#)

APC - The Association for Progressive Communications - [How to Avoid Becoming a Cyber-stalking Victim](#)