Blacklisting Email

When someone follows the instructions of a phishing email (clicking on a button without knowing the consequences, opening an unexpected attachment or sending someone your username and password), the problems begin. Immediately that information is collected and at a later time, often in the wee hours of the morning, the hacker logs into the compromised email account and starts sending out SPAM message after SPAM message, flooding the email lines with more phishing attacks coming from the compromised account.

Once the various email systems around the world start getting this SPAM, they recognize it as such and immediately blacklist the sending site where the SPAM is originating.

Blacklisting is a process of actively monitoring the Internet for reports of email traffic from a variety of sources sending unsolicited email (SPAM) and then publicly listing that known information on Internet sites for others to reference as a measure to fight SPAM. Many Internet Service Providers and independent organizations then use these blacklist databases as a filter applied to their inbound mail to prevent SPAM and to encourage internet security.

MORTON COLLEGE gets blacklisted when the SPAM originates from a MORTON COLLEGE compromised email account. The open-relay/proxy lists are the most widely used blacklists since they are based on the presumption that a "SPAMmer" found an email account and likely had relayed a high volume of SPAM through it, causing that email account to be reported to the list by recipients of that SPAM. Many of the better blacklists will run an automated script to verify that the evidence against that compromised email account is genuine before blacklisting the MORTON COLLEGE server. Many blacklists will quickly de-list the MORTON COLLEGE servers if IT submits a request to retest the "repaired" mail server. Of course, there will be time after you are de-listed (sometimes as long as a week), because the destination mail server administrators pull the updated lists at times they prefer.

Another method blacklist sites use to produce listings is that of "guilt by association". A blacklist site will list much larger blocks of accounts than those owned by the suspected abuser. This is where MORTON COLLEGE is most aggressively affected since a single compromised email account blocks all email coming from MORTON COLLEGE causing lots of bounced emails. Usually the reasoning behind this practice is that, by punishing innocent parties, the blacklister is putting more pressure on the Internet Service Provider to disconnect the suspected SPAMmer's Internet access. Usually this is a result of an email message header (@Morton College.edu) being connected to the SPAM.

The first clue that MORTON COLLEGE may have been blacklisted usually is that email senders will receive "bounce-back" emails from the destination to which they are attempting to deliver mail. Some of these bounce-backs will inform the email sender of the technical reason that they were blocked but some will not, depending on the preferences of the email recipients administrators.

Generally the most expedient way of being removed from a listing is to contact the blacklist directly. Since blacklisting services each have their own procedures for adding and removing offenders, all complaints are sent directly to the blacklisting service.

There are several ways to avoid being "blacklisted". MAINTAIN and update all anti-virus software. MORTON COLLEGE's anti-virus software manufacturer, Microsoft End Point, provides helpful information on virus definitions through a "threat list." New threats of viruses are listed on a daily basis, while other viruses are re-coded and re-distributed. Some of these viruses, called worm-viruses, are self-propagating infections that embed themselves into system files - causing the virus to send out SPAM, without anyone's knowledge, but that appears to come from your IP address.

DON'T SPAM!!! It is considered a violation of our Acceptable Use Policies and Guidelines to distribute unsolicited email. SPAMming is punishable by blacklisting, and has also been outlawed by many states.

Protecting MORTON COLLEGE from being blacklisted is everyone's responsibility. One compromised email account can cause countless problems and interrupt normal email traffic incoming and outgoing.

Again, please be vigilant of the email messages that land in your inbox – especially phishing messages that ask you to divulge personal information. **Morton College will NEVER send you an email asking you to divulge account details, or with links asking you to log into your account.** The easiest way to protect yourself is to never respond to anyone who asks for personal information by email, even it is from a seemingly legitimate source.

When in doubt contact helpdesk@morton.edu for a second opinion.