CHAPTER 2

Types of Malicious Messages

The introduction serves to illustrate the space of the problem. However, to understand what malicious messaging is, and what it is not, it is important to start with a specific definition. The definition offered here is the broadest possible, so that our explorations of the topic can include all possible dangers.

Malicious Message: A message in electronic form, mediated by automated information processing systems, that has been crafted or designed to assist in the achievement of a goal that is, in one or more ways, dangerous to the best interests of the recipient.

In simpler terms, it is an electronic message that can cause you, or the systems you are connected to, harm. There you have it: a short and to the point definition, that makes the point clear: you need to defend yourself against someone who intends to harm you. A tricky follow-on to that definition is figuring out what the potential scope of harm is. Can email harm you physically? Well, not by itself, since an email is nothing but a string of electrons. A properly crafted email may harm your computer, your data, or your network or any network to which you are connected. Additionally, a malicious email may possibly lead you into a situation in which physical harm is a possibility.¹

Herein lays the danger of malicious email: if simply opening an email can cause problems for you, how can you possibly know which emails are safe to open and which ones are not? Further, how can you know whether an attachment is safe to open or not? It is important to realize that there are no 100% solutions. In this book, we are going

¹ There is an important caveat to be added: while strings of electrons sent via message cannot harm you in 2014, they may well be able to harm you in the future, as technologies become even more interconnected with each other and with human support systems, such as medical equipment (pace makers, dialysis machines, insulin pumps, etc.) as well as potentially the human body itself. But that is beyond the scope of this exploration.
to review methods and techniques to give you a fighting chance in the ever escalating war between the senders and the receivers of malicious email.

We have set the stage for developing the skills to identify and combat quickly most malicious emails. Why only “most”? That is part of the problem, and is why education is so important: the attackers are constantly learning and refining their techniques to improve their chances of success. That is why the last chapter in this book covers what to do if one-or-more malicious emails successfully find their target. The target might not be you—it might be a colleague or a loved one, it may be a group you belong to, or it may be the resources and/or systems of your company. In any event, good preparations include not only preventing problems but also being ready to react should a problem occur.

A word closely associated with malicious messaging is “phishing.” This word is pronounced the same as the word “fishing” and it refers to a set of actions done to get victims to reveal sensitive information, such as bank account details, login credentials, passwords, or detailed personal information. In other words, the attacker is fishing for information. Phishing is closely associated with malicious messaging because the easiest way for attackers to execute this type of attack is by the use of messaging technologies, primarily email.

Recognizing that phishing is one of the great threats to an individual or institution, many researchers have set out to find an answer or create a tool that will prevent phishing attacks. Others have studied how the users can be better prepared to defend against such attacks, but nobody has done the research that ties it together into a holistic defense strategy. Some of this work brings together the research and practical knowledge assembled by many other sources, creating a unified framework for defending against phishing attacks. Through the fusion of various studies, a more robust and complete defense strategy can be created, and that through its implementation, individuals and organization will reduce the number of successful phishing attacks experienced annually. Until that work is completed and solutions are deployed, it is up to the individual user to understand and take steps to guard against these types of attacks.
In order to discuss malicious messages, I have divided the types into several categories of features. It is important to point out that these feature types are not exclusive: a malicious message can have several of the type features embedded in one message. However, in order to discuss the problem space, it is easier to separate and consider the problems individually. Once you know what the types of problems are, you are better able to recognize and avoid the problems.

It is important to point out that malicious messaging is not always spam, formally known as Unsolicited Commercial Email (UCE). UCE can clog your inbox, be very annoying, and steal time from more productive activities, but may not be malicious per se. Email and other forms of electronic messaging stray into the malicious zone when the purpose of the message goes beyond the simple advertising of a product. It can be very difficult indeed to differentiate annoying-but-legitimate unsolicited messages from malicious messaging. In fact, malicious email sometimes can even disguise itself as legitimate unsolicited messages in order to trick you into opening the email.²

Here are some examples of malicious email:

- invitations to participate in some activity, such as an employment scheme, that can result in theft of money (usually from the recipient);
- requests or demands to click on an embedded link, which results in your unwitting participation in fraudulent activity, such as traffic driving or click fraud, or your unknowing download of unwanted software or material, including viruses or pornographic material;
- requests or demands that attachments to the email be reviewed, where the attachment is malicious software that is executed when opened, embedding software in your computer.

These are but a few of the types of malicious email behavior seen. Rather than cataloging all types, we can generalize certain characteristics that can assist you in making the judgment call: “Is this email legitimate and is it safe to open?”

²The use of the term UCE rather than “spam” is to avoid the practice of confusing a food product with an interesting history, Spam, with the activities of mass marketers.
FEATURE TYPES OF MALICIOUS MESSAGES

The feature types of malicious messages are all intended to accomplish substantially the same purpose: to get the recipient to do something. The something can be responding to the email, clicking on an embedded link, or opening an attachment. Thus, we can quickly focus in on four primary feature types: appeals to emotion, trickery, subversive links, and subversive attachments. After describing the feature types, I have included real examples of actual emails that illustrate one or more of the feature types.

Appeals to Emotion

Emotion is a powerful motivator for human beings. Research has shown that emotional states can affect physical and mental health and can be responsible for hormonal changes in the body\(^3\). The sender hopes to get a recipient to act without considering if their emotions are being manipulated. Emotions that are common targets for bad guys to exploit include (but are not limited to) the following:

- emotions associated with comparative success, such as ambition, envy, narcissism, and greed;
- those associated with authority, such as intimidation, obligation, or pride;
- those associated with compassion, such as sympathy or kindness;
- those associated with paranoia, such as anger, bitterness, and fear; and
- those associated with community, such as courage and love.

Trickery

Disguising an electronic message to appear to be legitimate is an appallingy effective way to get recipients to do something they may not normally do. This approach is particularly effective when combined with an appeal to emotion. Often, these electronic messages include precise

copies of official logos, images, and other symbols of authenticity, such as trademark or copyright logos. The entire design of these types of messages is to convey an overwhelming sense of authenticity to the recipient so that trust will be implied. In addition, when that trust is effectively established through such trickery, the recipient’s defenses are reduced, thus increasing the probability that the goal of the sender will be accomplished.

Subversive Links
It is common to receive an electronic message with an embedded link to a website, a document, or some other asset. The problem is that these links are not always what they appear to be. It is possible to disguise a link to hide its true nature. For example, using appearance coding, a link to http://www.exampleofmaliciouslink.com could be disguised to look like something innocuous, like http://www.funwithpuppies.org. This is quite dangerous, as it can be difficult to discover what the actual link in the message is, depending on what platform the recipient is using to read messages. Some platforms, such as fully functioning desktop computers, provide enough functionality that users are able to look behind the curtain to discover the truth. Other platforms, such as some phones, have limited support to users to discover the true content of links. The purpose of subversive links is to get the recipient to load a website that then unleashes the attack on the recipient. Typically, this consists of downloading malicious software automatically. Because of this, a first order recommendation is never to click on a link in an electronic message. Instead, if you really feel like you need to find out what is at the link, use the various tricks at your disposal to discover the actual content. A few of these will be discussed later in the book, but a caveat remains that there are so many platforms, no discussion can possibly be complete and you should take a few minutes to find out how to do this on each of your devices. It is not difficult, as we will see, and can save you a world of pain.

Subversive Attachments
In a similar fashion, it is possible to disguise attachments to look quite legitimate. One common technique is to hide attachment file extensions (such as .doc or .txt) so that the recipient cannot easily detect that the attachment is actually an executable program. Double-clicking on the
attachment in the electronic message launches the file via the default application for that file type. Again, the first order recommendation is never to launch an attachment from within an electronic message. If you feel like you need to examine an attachment, you can save it to a protected area in your storage area and then use the directory listing to examine the file naming structure. To examine the contents of the file, you can use the File Open With command on your computer to look at the contents with a text editor, such as a note pad application. If you were expecting it to be a word processing document and all you see is a bunch of symbols or what appear to be hieroglyphs, then you know immediately that the file may not be what you expected it to be. If you are not able to ascertain to a reasonable level of certainty that it is a legitimate file, you should delete it. Alternatively, if you are in an enterprise environment, your network security people might want to examine the file.

A Further Complication
Rarely does the electronic mail have the return address of BadGuy@badguys.com. Instead, the sender identification will be designed to appear legitimate, innocuous, authoritative, or a combination of all those elements. A favorite trick is to use common names, so that the recipient will assume it is an acquaintance. In these days of social networks, where we have contact lists that number in the thousands, this type of disguise works fairly well to deceive the recipient. Another trick is to use the name of a celebrity or a slight variation on the name of a celebrity. The commonality of the name is such that the defenses of the recipient are reduced simply because the brain is tricked into a sense of normalcy. Electronic messages that are disguised to appear to come from authoritative sources, such as banks or government agencies, naturally have the sender identification modified to appear to be legitimate elements of the source.

All of these elements combine to create what can be an amazing array of tricks to deal with. The knowledge needed is simple, through awareness of the problem, a basic understanding of electronic messaging, and the development of a suspicious approach to electronic messaging. Then simply being cautious can provide an enormous amount of protection against these types of attacks.