alpha TECHNOLOGIES

SECURE IT

Sincerely, Malware. Recommendations For Securing Email

alpha TECHNOLOGIES

Tony Schliesser
Chief Information Security Officer

Organizations rely on email as a primary form of communications; both internally and externally. Whether it is to send an invoice, schedule a meeting, or collaborate internally; email for many businesses is an essential part of their day-to-day operations.

Most, however, do not realize that email is preferred method of attack by "hackers" used against organizations because of the level of insecurity in most email programs. For example, in a Phishing attack, an attacker creates convincing email messages (called Phishes) that trick the recipient into an action that the user would not normally do, like clicking a link to deliver Ransomware. As insecure as email is, we still use it for security related purposes such as recovering a forgotten password. So, how can we strengthen our email defenses?

Use Strong and Unique Passwords

A strong password is nearly impossible to guess without some insight. However, people are creatures of habit and remembering unique passwords is hard to do. As a result, people reuse passwords for websites and applications which provides the attacker with an advantage. When a website is compromised and passwords are leaked, this provides a list of passwords the attacker can try against the target email account. Using a password manager such as "1Password" or "Last Pass," helps protect against password reuse by making it easier to use strong unique passwords for all accounts and provides a secure place to store them.

Train Users: Security Awareness Programs

Every organization should consider a security awareness program that helps users identify phishing emails. In most cases, the success of phishing attacks can be reduced by training users on the tactics, techniques, and procedures used by attackers when conducting a phishing attack. Over time users become more adept at spotting phishing email, resulting in fewer compromises.

Use Multifactor Authentication (MFA) to Secure Email Accounts.

Multifactor authentication, better known as MFA, is a technique that uses something

in addition to a password to help prevent unauthorized access. For example, when logging into a bank account, many banks send a code via SMS to further validate the identity of the person accessing the account. This is an example of MFA. MFA provides an additional layer of defense to prevent unauthorized access in cases where the account passwords have been compromised from a data leak. Since the attacker would not have access to your phone in this example, access to your bank account would be denied. Email accounts are just as valuable as bank accounts since they can be leveraged to gain access to higher valued accounts.

Email Security Gateways

Email security gateways do more than limit the amount of spam (unsolicited commercial email) an organization receives. Email security gateways can also scan emails for malware, suspicious links, and in many cases will block most spoofed email. More advanced email security gateways can go a step further by "sandboxing attachments." Sandboxing attachments is a technique where attachments are examined in a "sandbox" to detect hidden malware before the message arrives in a user's inbox. Like most cybersecurity protections, email security gateways are not 100% perfect, but they do reduce the risks a user can face in their daily activities, as well as provides an additional layer of defense.

How Alpha Can Help:

Alpha understands how attackers use email to compromise an organization. We can help put the right defenses in place to reduce the risk of a successful attack, leaving your organization to do what it does best. For additional information on how to better protect our email services, or other security questions, please contact me.

Tony Schliesser - Chief Information Securtiy Officer
tschliesser@alpha-tech.us or salesgroup@alpha-tech.us
304-721-8625