Cybersecurity: Protecting You and Your Loved Ones Online

Online consumer threats are an unfortunate reality of our networked society and it seems as if malicious activity is accelerating, not receding. The good news is that there are tangible steps individuals can take to protect themselves against fraud, theft and property damage. Let's take at a high-level look at two common cybersecurity threats.

Malware

Malware is software intentionally designed to damage or disable a computer, server or system, and/or steal data or gain unauthorized access to networks.

How does this happen?

Malware may be installed on a user's computer when they innocently click an unsafe link, open an infected file, or visit a legitimate website that contains malware.

What harm can potentially result from malware?

Malware can delete files or directory information, or it may allow attackers to covertly gather personal data, including financial information and usernames and passwords.

How can I defend against malware threats?

Install the latest operating system and subsequent updates when prompted by your software provider. Installing anti-virus and anti-spyware software on all devices that connect to the Internet also adds a layer of defense. Norton and MacAfee are two highly regarded anti-virus software providers.

Phishing

Phishing occurs when cybercriminals pretend to be a trustworthy source to try and acquire sensitive personal information such as usernames, passwords, social security numbers, and credit card details.

How does this occur?

A seemingly legitimate email may instruct you to click on a link (e.g., "validate your account," "confirm your identity," "access your tax refund"). These links often connect to an illegal website that seeks personal information.

Why do people fall victim?

Because the cybercriminal masquerades as a legitimate source (e.g., bank employee, realtor), recipients may believe the request is valid.

What is the potential impact?

Malware may be installed on computer systems and personal identity details can be stolen.

How can I defend against phishing attempts?

The best defense involves recognizing common phishing indicators and carefully reviewing emails before clicking links or providing personal information.

- Take caution when receiving generic greetings such as "Dear Valued Customer," as these are often indicators of a phishing email.
- Beware of emails written with poor spelling, grammar and sentence structure.
- Ignore suspicious attachments, particularly when unsolicited and accompanied by a false sense of urgency.
- Hover over questionable links before clicking as this will reveal the true destination. Phishing emails will typically use a slight variation of a legitimate domain name (e.g. .net instead of .com).
- Trust your instincts. If an email or email attachment seems suspicious, don't open it. Emails offering money, threatening legal action or other alarmist messages are most likely illegitimate.

How can we help you? Please contact:
Jim O'Neil, Managing Director, 617-338-0700 x775
privateclient@appletonpartners.com
www.appletonpartners.com

APPLETON PARTNERS, INC.

Cybersecurity: Protecting You and Your Loved Ones Online

Proactive steps can be taken by individuals to help protect against cyber threats. Below we profile two such recommended "best practices" that can help reduce online risk.

Password Management

Passwords are intended to prevent unauthorized access to computer systems and accounts, although their effectiveness depends on how well they are created and protected.

What steps can I take to enhance password security?

Create passwords that are sufficiently long and reasonably complicated, as doing so makes it more difficult for hackers or other criminals to identify them. We recommend 8-12 characters with the use of upper and lower case letters, numbers, and symbols.

Never share your user name or password with anyone either verbally or by email. The easiest route to fraud is through password disclosure.

Change your password often – every 90 days is generally recommended.

Use a unique password for each account to prevent the potential of unauthorized access to multiple accounts should anyone gain access to any single account.

When shopping online, only do so on reputable web sites.

Multi-Factor Authentication

Multi-Factor Authentication is a security protocol in which a computer user is granted access only after successfully presenting two or more types of validation credentials. For example, a password and a code sent to your phone or email.

Why is Multi-Factor Authentication useful?

Requiring more than one set of credentials significantly decreases the probability that an attacker can impersonate a user and gain access to computers, accounts or other sensitive resources. Even if a criminal obtains your password, they are not likely to also have the second element needed to authenticate.

How does this relate to identity theft?

Identity theft is a very serious issue. By stealing your name, online credentials (e.g. user name, password) and other personal information, a criminal can potentially access your accounts and make illegal transactions such as purchases, cash withdrawals, or loan applications. MFA adds a valuable additional layer of security.

How do I set up Multi-Factor Authentication?

Most web sites that house sensitive personal information and require usernames and passwords offer an ability to implement MFA, although it is often referred to by different names. The process required to set up MFA is unique to individual web sites and may vary depending on how a site is accessed, but it typically involves following steps outlined within "Settings" and "Security". Directions for some of the more popular online destinations can be found here.

How can we help you? Please contact:
Jim O'Neil, Managing Director, 617-338-0700 x775
privateclient@appletonpartners.com
www.appletonpartners.com