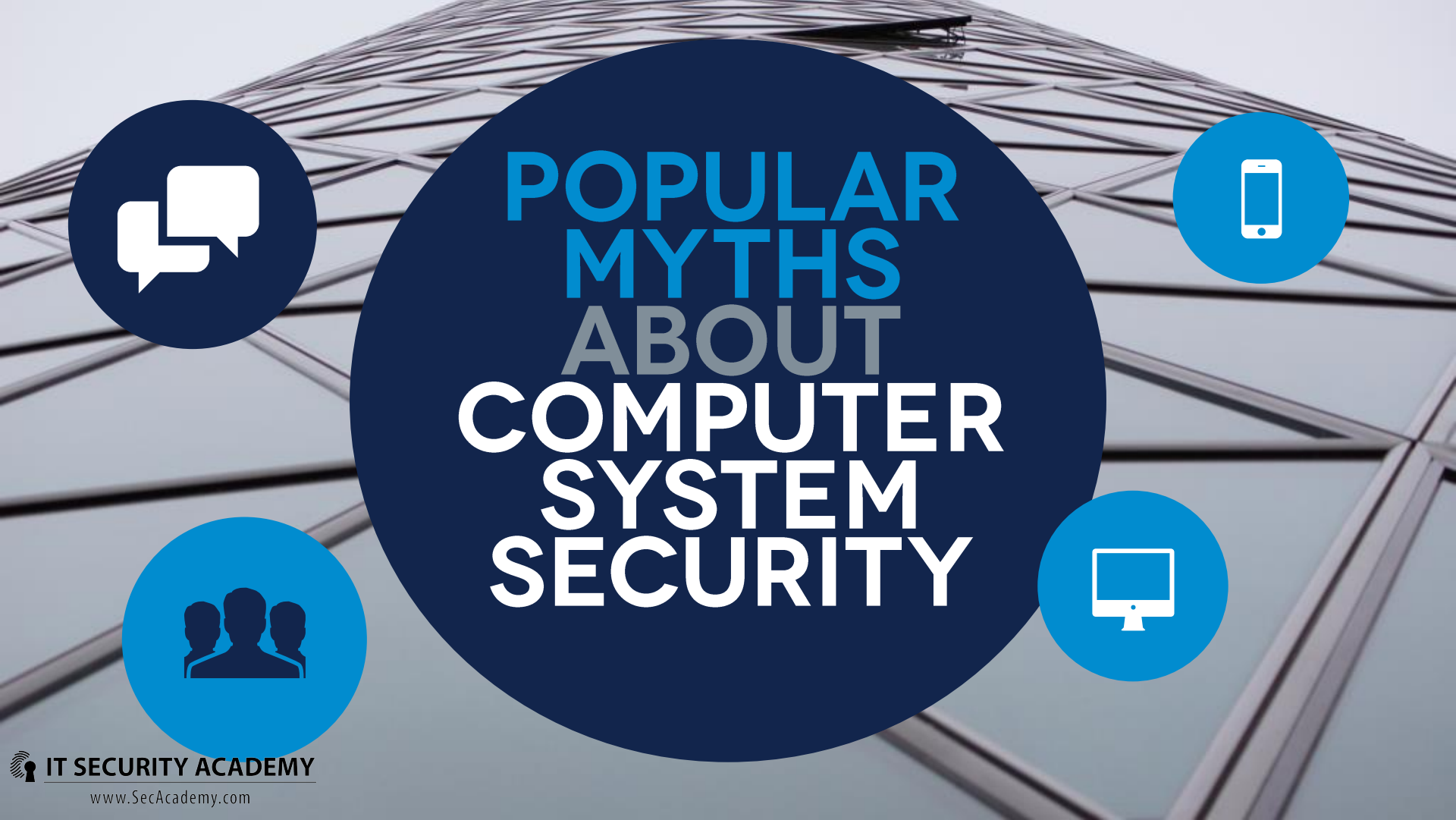
POPULAR
MYTHS
ABOUT
COMPUTER
SYSTEM
SECURITY
IT SECURITY ACADEMY
www.SecAcademy.com

ORIGINS

PCS HAVE TURNED 30 JUST RECENTLY:

The world's first 32-bit microprocessor was premiered by AT&T in 1980

The first IBM PC was created in 1981

THE HISTORY OF THE INTERNET STARTS IN 1968:

It was when APRPANET was created: the network joined four hosts located in Stanford, Los Angeles, Santa Clara and Utah

THE INTERNET AS WE KNOW IT ONLY CAME ABOUT IN 1990 WHEN TIM BERNERS-LEE DEVELOPED THE WORLD WIDE WEB.

ORIGINS

NEARLY ALL AVERAGE COMPUTER USERS AND EVEN PROFESSIONAL IT STAFFERS KNOW LITTLE ABOUT THE HOWS AND WHYS OF COMPUTERS AND COMPUTER NETWORKS, AND CAN'T USE THEM IN A SECURE WAY

They fill in the blanks by fostering these entirely wrong presumptions and myths about computer system and network security

POPULAR MYTHS

YOU CAN ENSURE TOTAL PROTECTION OF YOUR COMPUTER SYSTEM

A completely secure computer must not be connected to any network. It is not interactive and doesn't accept input. Also, you would need to bar users from installing any software, including the operating system

POPULAR MYTHS

NO-ONE WOULD EVER WANT TO ATTACK YOUR SYSTEM

Each computer and network can be targeted with a number of different attack techniques, ranging from the least sophisticated script kiddie attacks to professional intrusions launched by cyber criminals who make a living out of computer hacking.

POPULAR MYTHS

EFFECTIVE SECURITY IS ACHIEVED THROUGH OBSCURITY

Computer networks, including the Internet, use protocols that render effective obscurity infeasible. Even if you impair the functionality of your computer, intruders will still find a way to break into it

THANKS TO THE XYX TECHNOLOGY, YOU DON'T NEED PHYSICAL PROTECTION OR A SECURITY POLICY

People are denying the simple truth: any device or application can only protect you when it's turned on

POPULAR MYTHS

CLIENT-SIDE SECURITY SUCCESSFULLY PROTECTS SERVER

Whether it's a web server or database, any users have (or can easily obtain) full control over all applications running and started in their computer. To make matters worse, the data sent by the applications may be easily modified

CRACKING PASSWORDS IS THE BIGGEST THREAT

If an attacker intercepts an encrypted password used for authenticating a user in a system, they can masquerade as the user without needing to crack the password

POPULAR MYTHS

TOTAL COMPUTER SYSTEM SECURITY IS A PRIORITY IN ALL CASES

Total security is improbable for both computers and any other device or system. In nearly all cases, making computer systems totally secure is both impractical and commercially unviable

If you want total security, go to prison. There you're fed, clothed, given medical care and so on. The only thing lacking... is freedom.

Dwight D. Eisenhower

THANKS