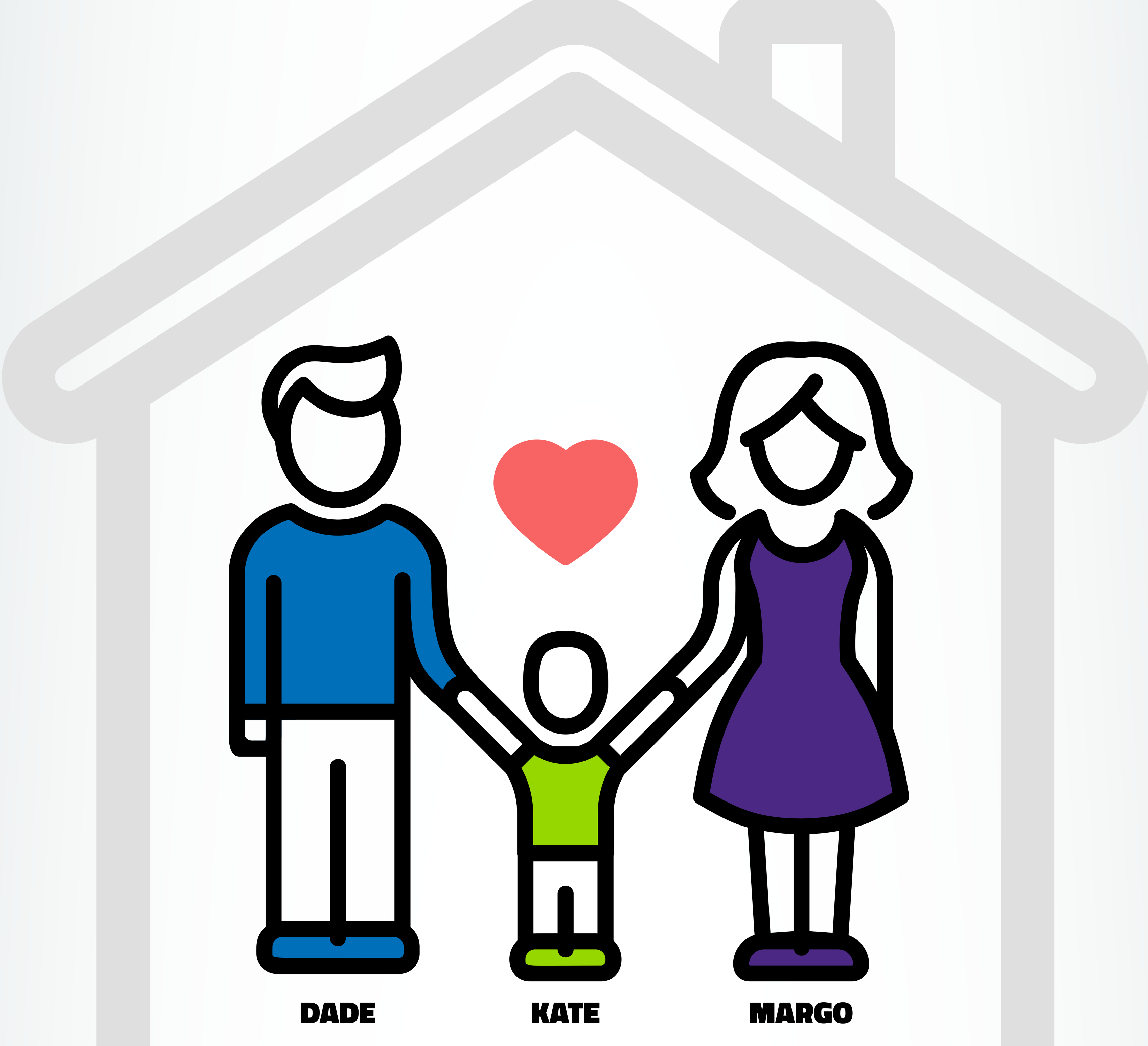
OCTOBER IS

NATIONAL CYBERSECURITY AWARENESS MONTH

Our world is more connected than ever, and that means we all play a role in making the internet a safer place to learn, connect, and do business. Here's an example of how every member of your family can play a part in the global spread of cyberattacks. Follow the safe habits below to stop cyber threats in their tracks.



Margo ignores a notification to download a software update, then visits a compromised website that quietly downloads a RAT (remote access tool) to her laptop via a malicious script in what is known as a drive-by attack.

Keep your software up to date, especially the most vulnerable apps, such as web browsers, PDF viewers, Adobe Flash, and Microsoft Office Also update any out-of-date browser extensions and add-ons.

In 2015, Oracle's Java posed the single biggest security threat to U.S. desktops, with 48% of users running outdated versions of the application[1].

Kate downloads a free game to her Android smartphone from the Google Play Store. Hidden malware inside the app infects Kate's device with a Trojan that goes undetected.

Android phones are especially vulnerable and should be running a trusted mobile security app. Routinely scan your device for malware.

A single piece of malware called 'Judy' infected as many as **36.5** million phones earlier this year[4].

The RAT connects to a command-and-control server, giving the attacker remote access to Margo's laptop. The attacker uses a keylogger to record her online banking password and steal her identity.

Make sure you have reliable, up-to-date antivirus software installed on all your devices to find and block threats such as banking Trojans.

A total of **$16 billion** was stolen from 15.4 million U.S. consumers in 2016[2].

After infecting Kate's phone, the Trojan accesses her contacts, sending a text message to her friends and family with a link to download the free game too.

Be cautious of the permissions you grant mobile apps. Malicious apps can spread when given access to your personal data, including your contacts and browsing history.

Allow TrojanOnWheels to access your Data?

ALLOW DENY

Margo uses that same banking password for her social media accounts, giving the attacker access to her Facebook. The attacker bulk messages Margo's friends a link to download the RAT, thus repeating the attack on hundreds of victims, bringing their devices into a botnet.

LOGIN

Use strong, unique passwords for all of your accounts and consider using a password manager. Closely monitor your social media accounts for any unusual activity, and don't click suspicious links in posts.

A 2013 study showed Facebook had 100 times more spam than other social networks and hosted **4 times** the number of phishing attacks[3].

In a matter of a few weeks, the Trojan has silently infected millions of Android devices around the globe, connecting them to the attacker's command-and-control server. This army of 'zombie' devices forms what is known as a botnet.

In the holiday season of 2014, a botnet was used to take down the PlayStation Network and Xbox Live via what is known as a distributed denial-of-service (DDoS) attack.[6]

The botnet is used to carry out a large-scale phishing attack targeting employees at companies around the world, including Dade's employer, IntiTech, Inc.

Businesses can thwart this type of attack by teaching their workforce how to identify phishing threats.

In 2016, the Necurs botnet used millions of infected devices to send out the massive malspam campaign behind the now-famous Locky ransomware.[7]

Dade receives a phishing email at his work address and downloads a .zip attachment containing a malicious Office file, allowing a ransomware payload to infect his work computer.

The ransomware infection spreads from Dade's computer to the company's network via a zero-day exploit. With the company's computers locked down, business grinds to a halt, affecting millions of customers worldwide.

Spot 'phishy' emails: Hover over email links to ensure the URL matches the actual hyperlinked address. Don't just trust the sender's displayed name. It's also a good idea to disable macros inside the Trust Center of your Microsoft Office programs.

Businesses can help prevent the spread of cyberattacks like ransomware by keeping their networked devices updated with the latest security patches.

As much as 93% of all phishing emails contain encryption ransomware[5].

The famous WannaCry ransomware attack in 2017 used a Windows exploit known as EternalBlue to quickly spread to networked computers in 150 countries.[8]

LEARN THE LINGO

Common cybersecurity terms you should know

Antivirus software is a program or set of programs designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.

A **bot** is an Internet-connected device that has been taken over and used to do something other than what was intended, usually via a remote access tool (RAT). Many bots are combined to form a **botnet**, which can be used to carry our different types of cyberattacks.

Command-and-control servers are used to issue commands to devices that are part of a botnet.

Firewalls act as protective barriers between computers and the internet. It is recommended you install them on your computers, laptops, tablets and smartphones, if available.

Hacking is the act of gaining unauthorized access into computer systems, usually in order to steal, change or destroy information, often by installing dangerous malware without your knowledge or consent.

Keyloggers are programs that record every keystroke made by a computer user, especially in order to gain fraudulent access to passwords and other confidential information.

Phishing is a social engineering hack that involves tricking people into revealing personal information, such as passwords and credit card numbers. These attacks are usually in the form of an email disguised as trustworthy.

Malware is short for "malicious software" and includes any program or file on a computer used to run unauthorized processes. Malware is used by cybercriminals to commit crimes such as identity theft and credit card fraud.

Ransomware is a type of malware that blocks access to your files until a "ransom" payment is made.

A **RAT** or **remote-access-tool** is a program used to remotely access or control a computer.

Trojans is a form of malware that misleads users of its true intent. Ransomware attacks are often carried out using a Trojan.

A **zero-day exploit** takes advantage of a security vulnerability in software before the software's creator becomes aware and fixes it.

[1] Java is the biggest vulnerability for US computers, by Maria Korolov. CSO Online, 1/26/2015
[2] 2017 Identity Fraud: Securing the Connected Life, by Al Pascual, Kyle Marchini, Sarah Miller. Javelin Strategy, 2/1/2017.
[3] STUDY: Facebook Has 100X More Spam Than Other Social Networks, 4X More Phishing Attacks, by David Chen. AdWeek, 10/1/2013.
[4] Android Malware 'Judy' Hits as Many as 36.5 Million Phones, by David Z. Morris. Fortune, 5/28/2017.
[5] 93% of phishing emails are now ransomware, by Maria Korolov. CSO Online, 6/1/2016.
[6] Infamous Lizard Squad attacks on Sony, Microsoft lead to federal charges, by Charlie Hill. Polygon, 10/7/2016
[7] Necurs Botnet Comes Back to Life After Three-Week Hiatus, by Catalin Cimpanu. Softpedia News, 6/22/2016
[8] Massive ransomware attack hits Europe, by Sara Fischer, Alayna Treene, and Shannon Vavra. AXIOS, 6/27/2016·