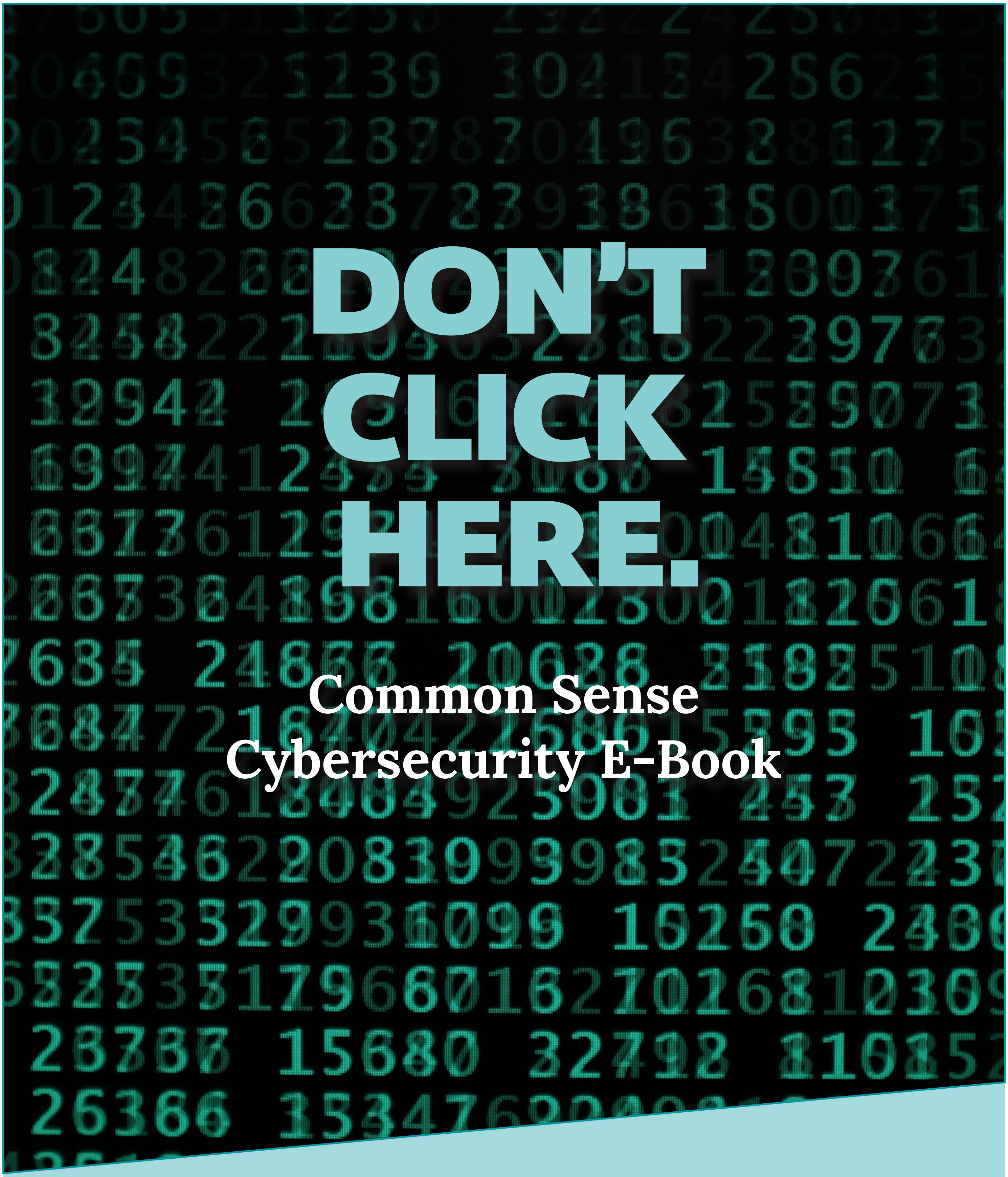


DON'T CLICK HERE.

Common Sense Cybersecurity E-Book

ENJOY SAFER TECHNOLOGY™

GOOD BOY. BAD PASSWORD.

When setting passwords remember—*fake it, mix it and manage it.*

Tip 1: FAKE IT

When you're prompted to give security answers based on personal information—your mother's maiden name, pet's name, first car, etc.—use fake answers. Real answers to personal security questions can easily be found by hackers through social media.

Tip 2: MIX IT

If you use the same password for access to all your accounts, you've made a hacker's job infinitely easier. Protect yourself by using unique passwords across all websites and apps that require opening a personal account with a password.

Tip 3: MANAGE IT

No one can accurately recall unique password credentials across dozens of separate accounts. That's why it's a good idea to use a password manager to securely store all of your various account passwords.

eset

It's not always this easy to tell real from fake.

DETER CYBERTHREATS IN DISGUISE WITH THESE TIPS.

Tip 1:
FILTER YOUR CONTENT.

Most organizations use some level of content filtering in the workplace and control those settings. But even at home, it's a good idea to use content filters to help protect yourself. Filtering pages can reduce malware exposure from risky sites.

Tip 2:
READ YOUR SEARCH RESULTS.

When searching online, be aware of websites and ads served in your search. Look carefully—they aren't always for the site, services or product you want.

Tip 3:
DON'T GO TOO DEEP.

Stick to the first page or two of your search results. That's where established, reputable companies and organizations will be. The deeper you go, the more likely you are to encounter risky sites.

ESET

THE SIGNS OFF MALWARE OUR EAZY TOO SPOT.

Identifying malware is the first step to avoiding it.

Step 1:
ALWAYS BE ALERT.

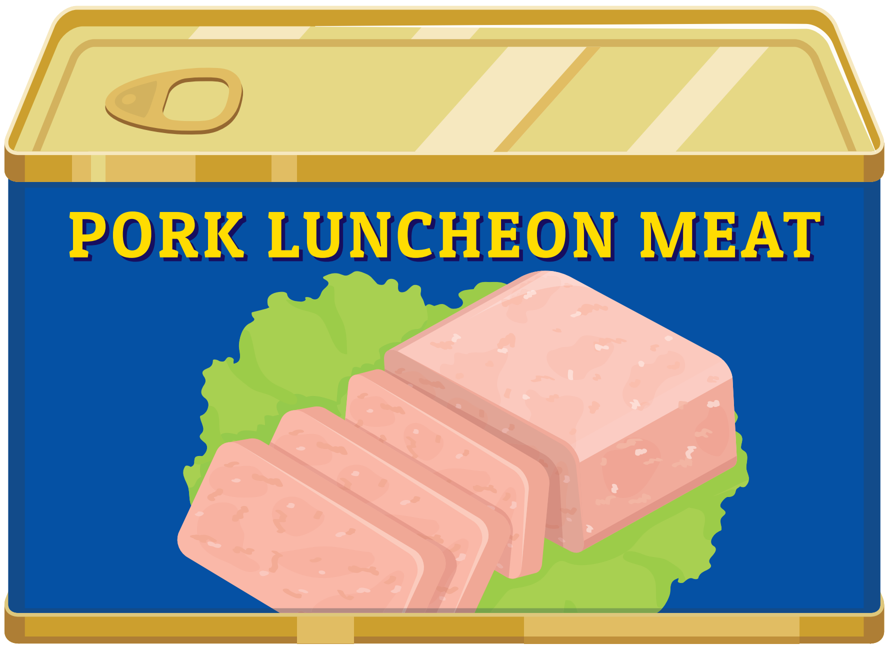
Make looking for signs of malware a habit. Watch out for common malware tip offs like poor spelling and grammar, URLs that seem suspicious, as well as prompts that use a strong sense of urgency to get you to click on a link.

Step 2:
CHECK YOUR CONTENT FILTERS.

At work, your organization likely has active content filters in place. It's also a good idea to use content filters at home. Because, if a risky email never reaches your inbox, you'll never accidentally click on a malicious link.

Step 3:
DON'T IGNORE SOFTWARE UPDATES.

Your IT department at work keeps your software up to date. It's a good idea to do the same on your devices at home. Keeping software and your OS current can help fix bugs as well as patch any known vulnerabilities that could be misused by cybercriminals looking for easy targets.



Don’t be fooled by a fake.

UNLESS IT COMES IN A TIN CAN, NEVER OPEN SPAM.

Tip 1:
THINK TWICE BEFORE YOU CLICK.

If an email, message, or other form of electronic communication is unsolicited and deceptive, then more than likely it is spam. Be extra cautious if an unsolicited message contains a link or attachment. Never download anything from an unknown source.

Tip 2:
KEEP YOUR PERSONAL DETAILS PERSONAL.

Never post your email or other personal information to public websites, apps or services. If you are asked for it, take the time to verify that the person or entity requesting your information is legitimate, and share it wisely.

Tip 3:
USE A DIGITAL “JUNK DRAWER.”

Create a disposable email address, which can be used for newsletters, subscriptions, surveys and receipts from online or in store purchases. This dramatically reduces your chance of being the target of harmful spam.

90% of malware is distributed by email and is often very inviting.

DON'T GET TRICKED BY MALWARE DISGUISED AS AN INVITATION.

Internal America Revenue

SEE SOMETHING PAY SOMETHING

Urgent! Response required.

Dear Taxplayer,

It has come to our attention that you are delinquent in your full tax payment for 2019. To avoid additional penalty fees, you must provide your SSN# immediately.

Click the link below to take care of it today, or else you'll be hearing from us again. Your wages could be garnished. And we're not talking about salt, pepper and a squeeze of lemon. We mean it. We're coming for you. Just click below to enter your SSN# and we can forget the whole matter.

Tax Filer reference: 123456789
Date received: 15 March 2019

Enter your SSN here: https://www.iard.gov.phished.hard

Internal America Revenue Department

Walla Walla, Washington
90210

Phishing only works when you're not paying attention.

Watch out for the top 3 phishing signs:

Sign 1:
TYPOS & ERRORS

Poor spelling and grammar and even incorrect logos are one of the first signs of a phishing attack. If you notice any obvious errors, be suspicious and extra careful.

Sign 2:
EMAIL DOMAIN

Look at the sender's domain email – does it match a known domain? An email domain is the part of an email address that comes after the @ symbol. Trusted companies are almost certain to have their own email domain. If you don't recognize the sender, read the subject line closely.

Sign 3:
UNKNOWN URLS

Is the URL correct? You can check this by hovering over the link in the email to see if it's from a site you know and trust. If the URL doesn't match the source of the email, don't click.

Without an "s" after http:, your safety is up in the air.

Tip 1:
ONLY SHARE INFO ON RELIABLE SITES.

Never enter personal information on a site (passwords, banking credentials, etc.) unless you are certain of its authenticity. Sites that use the https: protocol are typically safer—but to be sure, check the domain name carefully.

Tip 2:
BE WARY OF PUBLIC WI-FI.

Public wi-fi should always be treated as very insecure. Assume there could be hackers looking for an easy target on any public network. And never visit sensitive websites (banking, social media) when on public wi-fi. Use your phone's data service instead.

Tip 3:
LOOK FOR THE LOCK.

The lock icon in your browser tells you that the data transmitted between you and the site is encrypted, denying access to an outside third party. However, this does not guarantee a non-malicious site. It's always best to double check the domain name.

ENJOY SAFER
TECHNOLOGY™

www.eset.com