CYBERSECURITY AWARENESS MONTH

Do your part. #BeCyberSmart.

#BadJokes for Cyber Folks

Bad jokes can be so good. Enjoy a fun take on a serious topic with our best #BadJokes about cybersecurity.

Why did the chicken cross the node? To get to the endpoint on the other side.

Have you heard about the new Camo malware? It's really hard to detect.

A laptop and a desktop walk into an empty bar. The desktop sits down at a table. The laptop looks around angrily and shouts, "Where am I supposed to sit?!"

Did you hear about the man who used the factory password on his router? When his network got hacked, he got all the blame by default.

My friend has a real problem. She just can't stop herself from clicking on phishing emails. She's hooked!

When I was a kid, we used to worry about acid rain. With everything being uploaded to clouds nowadays, it's only a matter of time before we'll find ourselves drenched in data.

Don't be aware, be smart

At a time when we are more connected than ever, to say that practicing good digital hygiene is important would be a massive understatement.

Increasingly sophisticated cyberattacks and constantly evolving cybercriminals make daily attention to risk mitigation imperative. **It's not enough to be "cyber aware" anymore. Today, you must #BeCyberSmart.**

Each new connected device you use and online account you establish increases your attack surface and provides cybercriminals with another potential point of entry. And yet, the consistent practice of cybersecurity basics remains the most fundamental way to protect yourself and others.

Any device that connects to the internet is vulnerable to risks. **If you connect it, protect it.** The best defense is to keep your device's software, browser and operating system up to date.

#BeCyberSmart Tip: *When appropriate, turn on auto-updates.*

P@s$w0rds_d0n't_hav3_2_b_th!s_Complic@teD! **Use a phrase** to create a lengthy, unique and memorable password.

#BeCyberSmart Tip: *There's no one like you in the whole world – except a cybercriminal with your password. Don't get hacked. Use multi-factor authentication (MFA).*

Common sense plays a substantial role in maintaining good online hygiene. **Do your research before downloading new software or apps.** Consider the publisher's reputation, including user reviews and published articles.

#BeCyberSmart Tip: *Just because you don't use the software or app you installed doesn't mean that it's not using your device. Delete unused software/apps to increase the device's available space and reduce your attack surface. Win-win.*

Be diligent about **privacy and security settings,** including who can access your documents and devices. Take a few minutes to configure these settings before using new devices or accounts, and periodically revisit them to address possible changes.

#BeCyberSmart Tip: *For web meetings, require a password so only those invited can attend, and restrict screen and file sharing by attendees.*

No single tip is foolproof, but practicing them in parallel is the best way to maintain good online hygiene and protect yourself, and the people and networks with whom you connect, from cyberattacks.

Put #CybersecurityFirst for Privacy

Statistically, **phishing emails are the leading cause of data privacy incidents,** but stolen credentials, malware, denial-of-service (DoS) attacks, privilege abuse and mishandling of data are also common culprits.

As an employee, knowing how to identify potential threats to data privacy and understanding data handling best practices is not optional, **it's a responsibility.** Protecting your organization starts with you.

Put **#CybersecurityFirst** with the tips for preventing data compromise below.

HANDLE WITH CARE

Know and follow your organization's data retention policies. Data should be categorized, and access to sensitive data should be restricted to those who need it.

Minimize the number of places where confidential data is stored and keep track of where those places are. **Eliminate** any unnecessary data according to your organization's policies.

SAFEGUARD DATA

Secure important documents that could be stolen or copied. **Dispose** of confidential information by shredding or using software to permanently delete files from drives.

Portable devices like smart phones, laptops or USB drives are easily lost or stolen. **Ensure they are secured** with strong, unique passwords in the event they land in the wrong hands.

GET PERMISSION

Use only the devices, cloud services and software approved by your organization when completing work-related tasks.

Using unapproved applications or services could expose data, while connecting to your organization's network with an unapproved device could compromise the security of that network.

KEEP IT SEPARATE

Keep personal and business tasks separate. Personal internet browsing should be done on personal devices to protect the organization's devices and network.

Avoid using your business email to sign up for online services, newsletters or social media and **never use** the same credentials for multiple accounts to prevent credential theft.

#BECYBERSMART

Update software and devices regularly to patch security vulnerabilities.

Encrypt sensitive data before sending it via email.

Learn how to identify threats that attempt to gain your trust to obtain information like phishing, insider threats and social engineering.

The latest forecast estimates that global ransomware damage costs will reach $20 billion in 2021.

Data Risk Stats

Every organization is a potential target for data breaches and **every** organization collects and stores data that could be useful to a cybercriminal. And in most cases, secure systems cannot defend against **human error.**

So, how common, frequent and damaging are data breaches?

34%	of data breaches in 2018 involved internal actors
228	days to identify a breach in 2020, on average
$3.9	**million** – global average cost of a data breach
23%	of data breaches are caused by human error
39	seconds – how often a cyberattack occurs
38%	of users have a password that never expires
>1k	data breaches occur in the US alone each year
48%	of malicious attachments are Microsoft Office files
11	**million** – number of files a financial services employee can access

Source: Varonis
https://varonis.com/blog/data-breach-statistics/

Fight the Phish: Recognize red flags in malicious messages

Among other things, 2020 was an unprecedented year for cybercrime, with a **358% increase** in the distribution of malware compared to 2019.

Yet, for all the sophisticated, high-profile cyberattacks pulled off in the last year, it was phishing that truly thrived as the most popular attack vector, accounting for more than **80%** of reported security incidents.

The continued success of phishing as a threat vector is due in large part to **people like you.**

The unfortunate truth is that everyone is susceptible to fraudulent communications, **whatever the medium.**

Cybercriminals create elaborate emails, text messages and chat boxes that play on people's emotions to provoke a response, usually **opening a malicious attachment** or **clicking a link.**

For that reason, it's more important than ever to equip yourself with the knowledge necessary to **identify** these malicious messages.

When you receive any suspicious communications, **stop and think before you click.** Take one minute to review the message and search for any of the five common red flags shown below.

Taking just that extra minute to scrutinize that suspicious message may save you hours, days or even months of dealing with the **fallout** that comes from a compromised device or account.

Remember, if you have even the slightest suspicion that a message you received is phishing, **stop and think before you click.**

Red Flag #1

The sender of the message is unfamiliar to you, or the message is unexpected or oddly timed.

Watch out for:

- External senders
- Information you didn't request
- Messages outside normal hours

What it looks like:

- support@defendmail.net
- "Look at this document..."
- Sent at 2:04 a.m.

Red Flag #2

The sender's email address or the message itself contains odd spelling or grammatical errors.

Watch out for:

- Spoofed senders
- Unusual brand name style/usage
- Misspellings/unusual language

What it looks like:

- giftcards@arnazon.com
- "Your micro-soft login is disabled."
- "You're account is lock out."

Red Flag #3

The message urges actions like clicking links, opening attachments or replying with information.

Watch out for:

- Hidden link destinations
- Vague references to attachments
- Requests for information

What it looks like:

- "Click here to reset your password."
- "Please see attached."
- "What software do you use?"

Red Flag #4

The message appears to be time sensitive or threatens consequences for inaction.

Watch out for:

- Urgent requests
- Out-of-office-related requests
- Threats of legal action

What it looks like:

- "Please reply ASAP!"
- "I'm on vacation. Can you pay this?"
- "The authorities will be contacted."

Red Flag #5

The message contains links with shortened or mismatched URLs or attachments with odd file extensions.

Watch out for:

- Shortened or spoofed URLs
- Files containing macros
- Executable files

What it looks like:

- bit.ly/2KXjkLX or app1e.com
- .docm, .xlsm, .pptm, and more
- .exe, .bat, .bin, .msi, and more

According to Symantec, 1 out of every 4,200 emails sent during the first quarter of 2020 was a phishing email.

Who's Who: Cybersecurity Professions

A recent (ISC)^2 Cybersecurity Workforce Study revealed that the cybersecurity profession has a shortage of **more than four million people.** This is especially troubling when one considers that cybercrime is growing exponentially.

Cybersecurity professionals have skillsets that are **not only critical to business continuity,** but also **make a positive impact that extends beyond the digital world.** Not all cybersecurity professionals have a technical role. However, some of these technical roles are quite interesting.

The roles described below are only a sampling of the **dozens of different cybersecurity careers in the industry,** but they demonstrate how dynamic these roles can be.

While you may not be looking to change careers and become a cybersecurity professional, you can do your part to **#BeCybersmart** and help them help you.

Report suspicious emails, establish strong passwords and if you see something, say something.

Security Analyst

In this role, a professional often analyzes policies and protocols within the organization's systems and identifies areas of weakness. Armed with that information, they will customize the security technology to provide the organization the support it needs to remain secure.

Incident Responder

These professionals are the first responders to critical situations that occur within the organization. Think of them as firefighters for your organization's network. They quickly identify problems, contain them and apply changes so the problems don't occur again.

Penetration Tester

Often referred to as "ethical hackers," these professionals test the security of systems, technology and networks by trying to crack them with a particular objective (e.g., retrieve credit card information, compromise credentials of an executive, convince users to click on phishing links and download malware, etc). Their findings are outlined in a report provided to the organization, often including suggestions for remediation of discovered vulnerabilities.

Vulnerability Assessor

A penetration test looks at a particular scenario, while a vulnerability assessment is looking at all the discovered weaknesses (normally identified through a scan) in an organization's security. An assessor helps rank those issues for improvement.

Cybersecurity Roles

Do your part.
#BeCyberSmart.