IMCollaboration

Providing Technology and Cybersecurity Solutions

www.IMCollaboration.com
101 College Street
Dripping Springs, TX 78620

Andy Higgins, President

Monthly Update

August 2022

Back to School: Student Cybersecurity Tips

August 2, 2022 | Posted by Art Gross | Ransomware, Security

It's back-to-school time, and no matter the age of the student, or the location of the school, there's one class that everyone needs to pass. Smart cybersecurity habits need to be on all of our minds, and we can't afford to fail. We've put together some reminders about staying safe online and with your technology.

Before You Start Classes

Make sure that you're starting off the academic year on solid footing. Update all of your software and hardware to ensure that it has the latest security patches installed. If you are using an outdated version or technology, consider an upgrade that is equipped with stronger defense mechanisms against cybercrime. There are many student discount options available. Some may not be promoted, so ask at the store or do a bit of research online before you shop. Many reputable vendors have student options. When you are downloading software updates, only do it from the manufacturer's site. Turn on automatic security updates.

Purchase a charging block to avoid the need for public charging devices or stations. These are

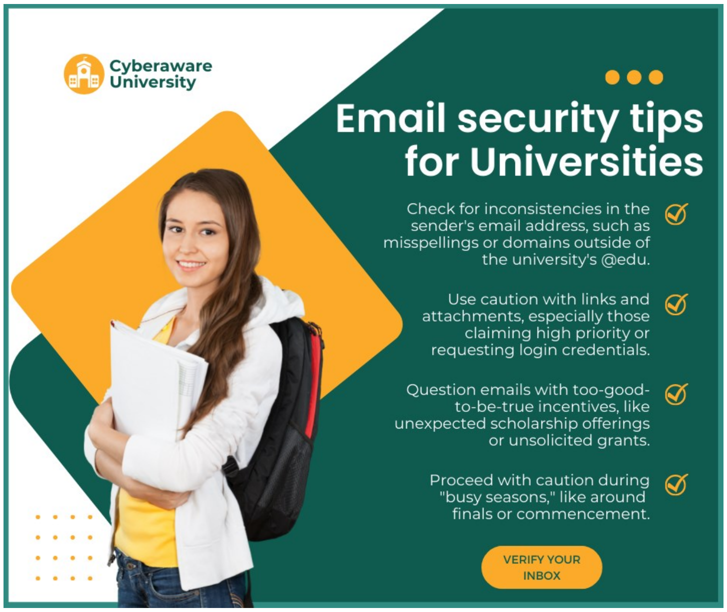
(Story continues on page 2)

often the source of detrimental downloads and can easily be avoided with your own equipment.

Password security should be taken seriously. Review your passwords and use a password manager to store your secure login credentials. Review your laptop settings and make sure that the screen locks after inactivity. Enable options that would allow you to locate your device or wipe the data if it is stolen. You can also use security tracking tags on hardware.

Review your banking credentials to have multi-factor authentication and enable alerts for suspicious spending.

Students are a target demographic. Be wary of "free" offers or job scams that require you to pay for them. You should be paid to work, not the other way around. Consult with your school administration about employment or intern programs in order to verify legitimacy.



Cyberaware University

Email security tips for Universities

Check for inconsistencies in the sender's email address, such as misspellings or domains outside of the university's @edu. ✓

Use caution with links and attachments, especially those claiming high priority or requesting login credentials. ✓

Question emails with too-good-to-be-true incentives, like unexpected scholarship offerings or unsolicited grants. ✓

Proceed with caution during "busy seasons," like around finals or commencement. ✓

VERIFY YOUR INBOX

Class Is In Session

You'll be forging many new relationships both academically and socially. Be aware of email phishing scams and fraudulent email addresses. Don't click on links before verifying that the sender is legitimate and not a spoofed address

Miscellaneous Cyber Safety

While these aren't hardware related, be aware of cyberbullying and how much you share online. Location services can be a valuable tool if in the hands of people that you trust. And while cyberbullying isn't something you can prevent with a download, you can be aware of it.

Free Report Download:
The Business Owner's Guide To IT Support Services And Fees

IT BUYERS GUIDE

What Every Business Owner MUST Know About IT Support Services And Fees

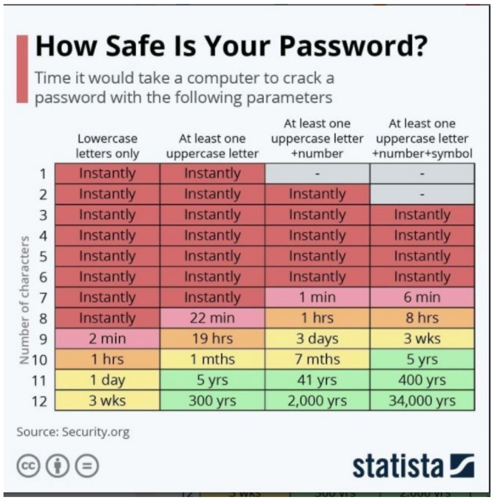
What You Should Expect To Pay For IT Support For Your Business And How To Get Exactly What You Need

You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.

Claim your FREE copy today at www.IMCollaboration.com/ITbuyersguide

Strong password behavior is the foundation of many aspects of a cybersecurity program. There are still people that have the same password for all their accounts. As an MSP, we are not present when passwords are created or oversee the process. But we can provide education that provides essential knowledge and encourage users to utilize good cyber aware habits.



How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

statista

Two-Factor Authentication (2FA)

At IMCollaboration we strongly recommend that users move towards implementing Two-Factor Authentication in any software or service it is available. Did you know that many email services allow you to add this security feature? Even Facebook has made the option for a 2FA/MFA (multi-factor authentication) available.

The Adventures of Cyber Cat
MY PASSWORD IS PURRRFECT
EASY TO REMEMBER AND UNIQUE TO ME
IT'S MITTENS1!

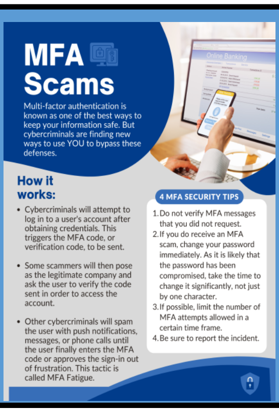
Implementing 2FA/MFA can add an additional layer of protection even if your password is not as strong as it should be, but creating a very strong password with authentication can provide a sense of relief.

The Adventures of Cyber Cat
Mittens, get off of my laptop!
I can't! I must protect Human from brute-force attacks.
But, I use multi-factor authentication to reduce my risk of a security breach.
Welp, my work here is done...

IMCollaboration partners with industry leaders to make our clients' businesses more secure. Nevertheless, if an employee uses the same password in their personal technology with internet access, your business could become vulnerable if that user becomes a victim of cyber criminals. This is why we have made providing your business employees with state-of-the-art training a priority.

As an IMCollaboration customer, we can provide your business with: Initial Cybersecurity Assessments of New Employees, Annual Cybersecurity Training and Weekly Micro-training for all employees. If you are a current customer and not utilizing this service, contact us today and we can get you set up. If you are not a current client and your MSP is not supplying this service, we can provide a FREE Dark Web Scan and Cyber Security Assessment to help identify your businesses vulnerabilities.

IMPORTANT NOTE: Although 2FA/MFA is a tool that adds enhanced cybersecurity protections, beware of possible scams:



MFA Scams

Multi-factor authentication is known as one of the best ways to keep your information safe. But cybercriminals are finding new ways to use YOU to bypass these defenses.

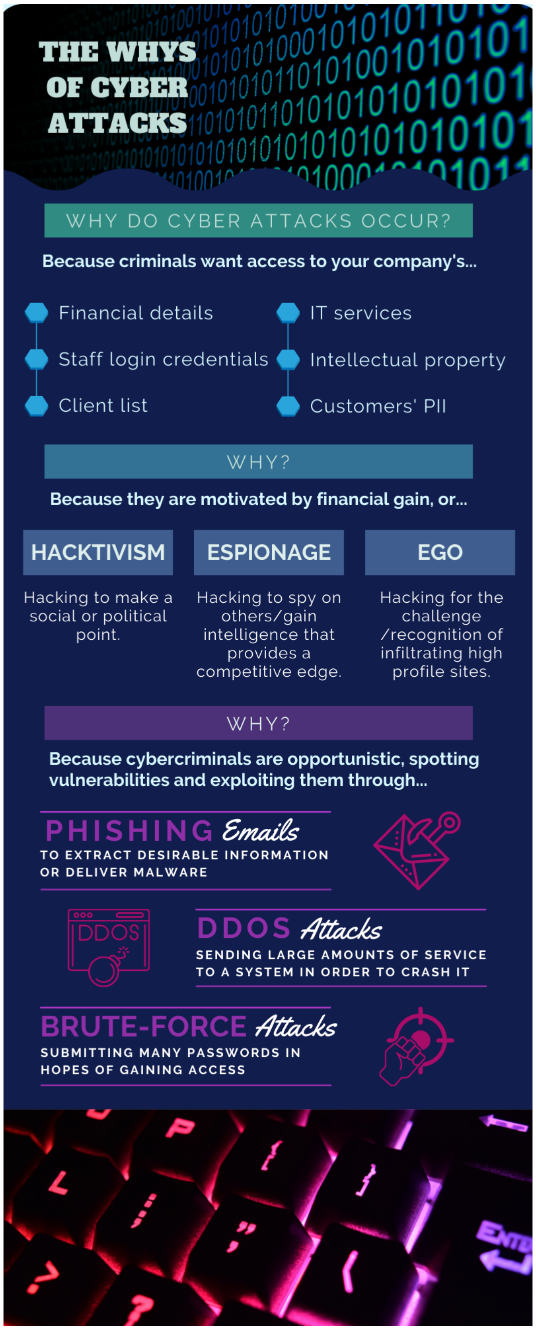
How it works:

- Cybercriminals will attempt to log in to a user's account after obtaining credentials. This triggers the MFA code, or verification code, to be sent.
- Some scammers will then pose as the legitimate company and ask the user to verify the code sent in order to access the account.
- Other cybercriminals will spam the user with push notifications, messages, or phone calls until the user finally enters the MFA code or approves the sign-in out of frustration. This tactic is called MFA Fatigue.

4 MFA SECURITY TIPS

1. Do not verify MFA messages that you did not request.
2. If you do receive an MFA scam, change your password immediately. As it is likely that the password has been compromised, take the time to change it significantly, not just by one character.
3. If possible, limit the number of MFA attempts allowed in a certain time frame.
4. Be sure to report the incident.

Cybersecurity Threats Are Real



THE WHYS OF CYBER ATTACKS

WHY DO CYBER ATTACKS OCCUR?

Because criminals want access to your company's...

- Financial details
- Staff login credentials
- Client list
- IT services
- Intellectual property
- Customers' PII

WHY?

Because they are motivated by financial gain, or...

HACKTIVISM
Hacking to make a social or political point.

ESPIONAGE
Hacking to spy on others/gain intelligence that provides a competitive edge.

EGO
Hacking for the challenge /recognition of infiltrating high profile sites.

WHY?

Because cybercriminals are opportunistic, spotting vulnerabilities and exploiting them through...

PHISHING *Emails*
TO EXTRACT DESIRABLE INFORMATION OR DELIVER MALWARE

DDOS *Attacks*
SENDING LARGE AMOUNTS OF SERVICE TO A SYSTEM IN ORDER TO CRASH IT

BRUTE-FORCE *Attacks*
SUBMITTING MANY PASSWORDS IN HOPES OF GAINING ACCESS

IMCollaboration

.....A look inside our business

Our Technical Support Team Continues to Grow. Please Meet Joseph Fryer

We understand that our clients expect and deserve quick resolution to all their technology needs. By adding to our technical support team, we can continue to respond quickly while expanding our ability to tackle those longer client technical projects.

Scan the barcode to request a Cybersecurity Assessment and Dark Web scan for your business