

# Cyber >>> Safety Tips



## Never share your password to anyone.

Keep your passwords safe.  
Use a secure and reliable password manager.

## Practice safe browsing.

A single careless click can expose your sensitive information. Think before you click!

## Verify Email Senders

Before you respond, verify the address of the person you're sending email to.

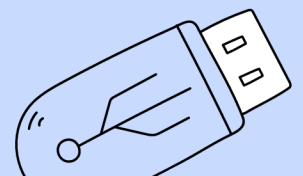
## Report Suspicious Events

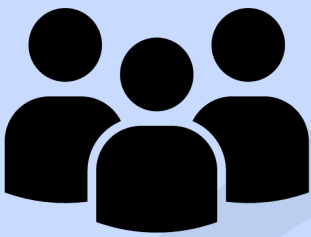
Contact CodeBlue in the event of something suspicious.  
(804) 521-7660

## Inspect Links in Email

Microsoft.com and MicrOsoft.com look similar. Threat actors use these tricks to get information from you.

**Stay safe online!**





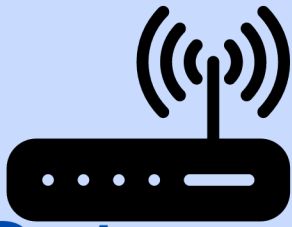
## End Users Security

- Awareness and training
- Education and real-time updates
- Remote and On-Site support



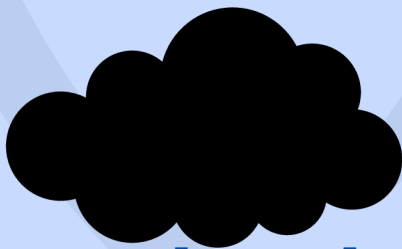
## Computer Security

- End-Point Security Software
- Software Patching and Maintenance
- Data Backup, Ransomware Protection



## Gateway Security

- Traffic inspection and detection
- Hardware Monitoring and Updates
- Zero-Day Patching of Security
- HIPAA Compliance



## Cloud Security

- Data at Rest Protection
- Cloud Data Backup
- Email Security and continuity
- HIPAA compliance



## The top 5 most reported cybersecurity breach entry methods

### Phishing Attacks

Cybercriminals use fraudulent emails, texts, or websites to trick individuals into revealing sensitive information like passwords or credit card details.

### Malware (Including Ransomware)

Malicious software such as viruses, trojans, or ransomware is used to gain unauthorized access to networks, steal data, or encrypt files for ransom.

### Weak or Compromised Passwords

Hackers exploit weak, reused, or default passwords to gain access to accounts or networks, often using brute-force attacks.


### Unpatched Software Vulnerabilities

Failure to update software or apply security patches leaves systems exposed to known vulnerabilities that hackers can exploit.

### Insider Threats

Employees or contractors, either maliciously or unintentionally, can compromise systems by mishandling data, misconfiguring systems, or leaking information.

---




**From:** WellsFargo - Support\_Online <WellsOnlineBank2@comcast.net> **1**

**Date:** December 8, 2017 at 2:23:01 PM EST

**To:** Undisclosed-Recipients;;

**Subject:** !Alerts! **2**

---

 [wellsfargo.com](http://wellsfargo.com)

---

**Security Information Regarding Your Account.**

We are sorry, **For your protection and security reasons,** your Wells Fargo account has been locked. **2**

Please click on the following link to unlock your account.

**Log-in to :<https://www.wellsfargo.com/online-banking/updating>** **3**

Thank you for bringing this matter to our attention.

Sincerely,  
Wells Fargo Online Banking Team.

---

[wellsfargo.com](http://wellsfargo.com) | [Fraud Information Center](#)

## What is Vishing and how to prevent it

**Vishing** is a crime involving personal information being stolen over the phone.

Some callers try building trust and then request bank information, passwords, etc.

Others leave intimidating voice mails that threaten with fines or jail to make someone give up their information.

Never give personal information over the phone



Always ask them to verify their identity or give proof



Don't answer messages asking for your phone number



Phone calls and texts are as prevalent

# Email Isn't All

## What is Smishing and how to prevent it

**Smishing** is a cybercrime where personal information is stolen over text message.

Scammers utilize the lack of skepticism and awareness about smishing to deceive.

Texts seem personal, relevant and urgent which makes victims feel compelled to respond.

If in doubt, contact the bank or company directly



Don't answer suspicious text messages



Be cautious if a text warrants an urgent response

